Euler and Wilson’s Theorem Solutions

Justin Stevens

Problem 1. (AIME) The positive integers \( N \) and \( N^2 \) both end in the same sequence of four digits \( abcd \) when written in base 10, where digit \( a \) is not zero. Find the three-digit number \( abc \).

Solution. We can rewrite the given condition as

\[ N^2 \equiv N \pmod{10,000} \implies N(N - 1) \equiv 0 \pmod{10,000}. \]

We therefore have two separate cases, since \( N \) and \( N - 1 \) are relatively prime:

\[
\begin{align*}
N &\equiv 0 \pmod{625} \quad \text{and} \quad N 
&\equiv 1 \pmod{16} 
\implies N \equiv 625 \pmod{10,000}; \\
N &\equiv 1 \pmod{625} \quad \text{and} \quad N 
&\equiv 0 \pmod{16} 
\implies N \equiv 9376 \pmod{10,000}.
\end{align*}
\]

Since \( a \) is nonzero, we must have \( N \equiv 9376 \pmod{10,000} \), therefore \( abc = 937 \).

Problem 2. (1999 AHSME) There are unique integers \( a_2, a_3, a_4, a_5, a_6, a_7 \) such that

\[
\frac{5}{7} = \frac{a_2}{2!} + \frac{a_3}{3!} + \frac{a_4}{4!} + \frac{a_5}{5!} + \frac{a_6}{6!} + \frac{a_7}{7!}
\]

where \( 0 \leq a_i < i \) for \( i = 2, 3, \ldots, 7 \). Find \( a_2 + a_3 + a_4 + a_5 + a_6 + a_7 \).

Solution. Multiply out by the least common denominator, \( 7! \), to see

\[
5 \cdot 6! = a_2(7 \cdot 6 \cdot 5 \cdot 4 \cdot 3) + a_3(7 \cdot 6 \cdot 5 \cdot 4) + a_4(7 \cdot 6 \cdot 5) + a_5(7 \cdot 6) + a_6 \cdot 7 + a_7.
\]

Reducing modulo 7 and using Wilson’s Theorem, we see \( a_7 \equiv 5 \cdot 6! \equiv 5 \cdot (-1) \equiv 2 \pmod{7} \). Since \( 0 \leq a_7 < 7 \), \( a_7 = 2 \). Subtracting 2 and taking the equation modulo 6 gives

\[
5 \cdot 6! - 2 = a_2(7 \cdot 6 \cdot 5 \cdot 4 \cdot 3) + a_3(7 \cdot 6 \cdot 5 \cdot 4) + a_4(7 \cdot 6 \cdot 5) + a_5(7 \cdot 6) + a_6 \cdot 7 \equiv a_6 \pmod{6}.
\]

Therefore, \( a_6 \equiv -2 \equiv 4 \pmod{6} \), so \( a_6 = 4 \). Subtracting 28 from both sides gives

\[
5 \cdot 6! - 30 = a_2(7 \cdot 6 \cdot 5 \cdot 4 \cdot 3) + a_3(7 \cdot 6 \cdot 5 \cdot 4) + a_4(7 \cdot 6 \cdot 5) + a_5(7 \cdot 6).
\]

Taking the equation modulo 5, we see \( a_5 = 0 \). Dividing both sides by \( 7 \cdot 6 \cdot 5 = 210 \),

\[
17 = 12a_2 + 4a_3 + a_4 \iff (a_2, a_3, a_4) = (1, 1, 1).
\]

Therefore, \( a_2 + a_3 + a_4 + a_5 + a_6 + a_7 = 1 + 1 + 1 + 0 + 4 + 2 = 9 \).
Problem 3. Determine the greatest common divisor of the elements of the set

\[ S = \{ n^{13} - n \mid n \in \mathbb{Z} \}. \]

Solution. We determine all primes \( p \) such that \( p \mid n^{13} - n \) for every \( n \). If \( \gcd(n, p) = 1 \), then by FLT, \( n^{p-1} \equiv 1 \pmod{p} \). Also \( n^{12} \equiv 1 \pmod{p} \), therefore \( p - 1 \mid 12 \). The possible primes are hence \( p \in \{2, 3, 5, 7, 13\} \). Furthermore, \( p^2 \) does not divide the element \( p^{13} - p \). Therefore the greatest common divisor of \( S \) is \( 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 = 2730 \). \( \square \)

Problem 4. Find the last 8 digits in the binary expansion of \( 27^{1986} \).

Solution. We wish to find the number modulo 256. Since \( \phi(256) = 128 \),

\[ 27^{1986} \equiv 27^{1986} \pmod{128} \equiv 27^2 \equiv 729 \equiv 217 \pmod{256}. \]

Converting this number to binary, we see \( 217 = 128 + 64 + 16 + 8 + 1 = 11011001_2 \). \( \square \)

Problem 5. A repunit is a number consisting only of the digit 1, such as 111 and 11111.

(a) Let \( n \) be a number relatively prime to 10. Prove that there is a repunit divisible by \( n \).

(b) Find the smallest repunit divisible by (i) 21 (ii) 19.

Solution. (a) Let a repunit with \( j \) digits be denoted \( a_j \). Assume that there are no repunits divisible by \( n \), hence there are \( n - 1 \) possible remainders when we divide \( a_j \) by \( n \). Considering an infinite number of repunits by the pigeonhole principle, two must have the same remainder upon division by \( n \), say \( a_i \) and \( a_j \) for \( j > i \). However, then

\[ a_j - a_i = \underbrace{111 \cdots 111}_{j \ 1's} - \underbrace{11 \cdots 11}_{i \ 1's} = 10^i \cdot \underbrace{11 \cdots 11}_{j-i \ 1's} = 10^i a_{j-i}. \]

Since \( \gcd(n, 10) = 1 \) and \( a_j \) and \( a_i \) have the same remainder, \( n \mid a_{j-i} \), contradiction. We can therefore always find a repunit divisible by \( n \).

(b) (i) The repunit must have a multiple of 3 digits. By FLT,

\[ 11111 = 10^5 + 10^4 + 10^3 + 10^2 + 10 + 1 = \frac{10^6 - 1}{9} \equiv 0 \pmod{7}. \]

Since \( 10^3 \equiv -1 \pmod{7} \), this is the smallest repunit divisible by 21.

(ii) By the geometric series formula, the formula for a repunit with \( N \) digits is

\[ \underbrace{111 \cdots 111}_{N \ Y's} = \sum_{k=0}^{N-1} 10^k = \frac{10^N - 1}{9}. \]

By FLT, \( 10^{18} \equiv 1 \pmod{19} \), therefore the smallest \( N \) must be a divisor of 18. Testing the divisors, \( 10^2 \equiv 5 \pmod{19 \), \( 10^3 \equiv 12 \pmod{19 \), \( 10^6 \equiv 11 \pmod{19 \), and \( 10^9 \equiv 18 \pmod{19} \). Since no divisor works, the smallest \( N \) is \( N = 18 \). \( \square \)
Problem 6.  (a) The Fermat numbers are defined by \( f_n = 2^{2^n} + 1 \) for integer \( n \). Prove that the Fermat numbers are pairwise relatively prime, that is \( \gcd(f_n, f_m) = 1 \) for \( n \neq m \).

(b) Prove that every composite Fermat number is a base-2 pseudoprime.

Solution.  (a) WLOG \( n > m \). Repeatedly using difference of squares,

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

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

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

\[
= \cdots
\]

\[
= f_{n-1} f_{n-2} f_{n-3} \cdots f_1 f_0
\]

Hence \( f_n \equiv 2 \pmod{f_m} \). By the Euclidean Algorithm, \( \gcd(f_n, f_m) = \gcd(f_m, 2) = 1 \).

(b) Since \( f_n = 2^{2^n} + 1 \), \( 2^{2^n} \equiv -1 \pmod{f_n} \). Raising this to the \( 2^{2^n-n} \)th power,

\[
2^{f_n-1} = 2^{2^{2^n}} = (2^{2^n})^{2^{2^n-n}} \equiv (-1)^{2^{2^n-n}} \equiv 1 \pmod{f_n}.
\]

By definition, this congruence implies \( f_n \) is a base-2 pseudoprime.