In this exam all variables are integers. Solutions mean integer solutions.

1. (25 points)
   (1) Let \( d = \gcd(231, 175) \). Find \( w \) and \( z \) such that \( 231w + 175z = d \).
   (2) Find a complete set of mutually incongruent solutions of
      \( 231x \equiv 28 \pmod{175} \).

2. (25 points) Recall that Fibonacci numbers are defined as \( F_1 = 1 \), \( F_2 = 1 \) and \( F_{n+2} = F_{n+1} + F_n \) for all \( n \geq 1 \). Show that
   \[
   F_1 + 2F_2 + 3F_3 + \cdots + nF_n = nF_{n+2} - F_{n+3} + 2
   \]
   for all \( n \geq 1 \).

3. (25 points) Let \( p > 2 \) be prime. Let \( \{a_1, a_2, \ldots, a_{p-1}\} \) be a reduced residue system modulo \( p \). Which of the following are also reduced residue system modulo \( p \)? For each part, if the answer is always yes or no, explain why; if it is sometimes yes and sometimes no, give an example for each case.
   (1). \( \{a_1^3, a_2^3, \ldots, a_{p-1}^3\} \).
   (2). \( \{b_1, b_2, \ldots, b_s\} \) where each \( b_i = \sum_{j \neq i} a_j \) (i.e, \( b_i \) is the sum of all \( a_j \) except \( a_i \)).
   (3). \( \{a_1^k, a_2^k, \ldots, a_{p-1}^k\} \). Here \( 1 \leq k \leq p-1 \) and \( \gcd(k, p-1) = 1 \).

4. (25 points) Find the least positive integer \( n \) that satisfies
   \[
   101^{304} \equiv n \pmod{13}.
   \]

Solutions on next page
Solutions:

1. (1). Direct computation shows $d = 7$. One combination is $231 \times (-3) + 175 \times 4 = 7$.

   (2). Since $7 \mid 28$. The equation $231x + 175y = 28$ has solution. One solution for $x$ is $x = -12$ (multiple the solution in (1) by $\frac{28}{7} = 4$). Therefore a set of mutually incongruent solutions for $231x \equiv 28 \pmod{175}$ is $-12 + t \cdot \frac{175}{7} = -12 + 25t$ where $0 \leq t \leq 6$.

2. Use Induction. Check it is true for $n = 1$. Assume it is true for $n$, then by induction $F_1 + 2F_2 + 3F_3 + \cdots + nF_n + (n+1)F_{n+1} = nF_{n+2} - F_{n+3} + 2 + (n+1)F_{n+1} = (n+1)(F_{n+1} + F_{n+2}) - (F_{n+2} + F_{n+3}) - 2 = (n+1)F_{n+3} - F_{n+4} - 2$.

3. Not always true. For example if is true if $p = 5$, but false if $p = 7$. See (3) below.

   (2). Yes. By #4 in §5.2, $\sum_{i=1}^{p-1} a_i \equiv 0 \pmod{p}$. Therefore $\sum_{j \neq i} a_j \equiv -a_i$, and it is clear $-a_1, -a_2, \cdots, -a_{p-1}$ is also a reduced residue system modulo $p$.

   (3). Yes. The only thing need to check is all $a_i^k$ are mutually incongruent. Assume $a_i^k = a_j^k$. Note $a_i^{p-1} \equiv 1$ by Fermat’s Theorem. Since $\gcd(k, p-1) = 1$, there exists $a$ and $b$ such that $ak + b(p-1) = 1$. If $a > 0$, then $b < 0$. So

   $$a_i \equiv a_i^{1+(p-1)(-b)} \equiv (a_i^k)^a \equiv (a_j^k)^a \equiv a_j^{1+(p-1)(-b)} \equiv a_j.$$  

   So $i = j$. If $a < 0$, then $b > 0$, similarly we have

   $$a_i \cdot (a_i^k)^{-a} \equiv (a_i^{p-1})^b \equiv 1 \equiv (a_j^{p-1})^b \equiv a_j \cdot (a_j^k)^{-a} \equiv a_j \cdot (a_i^k)^{-a}.$$  

   Therefore $a_i \equiv a_j$ since $\gcd((a_i^k)^{-a}, p) = 1$.

4. We have $101 \equiv -3 \pmod{13}$. By Fermat’s Theorem $(-3)^{12} \equiv 1 \pmod{13}$. Note $304 = 12 \cdot 25 + 4$. So

   $$101^{304} \equiv (-3)^{304} \equiv ((-3)^{12})^{25} \cdot (-3)^4 \equiv 1 \cdot 81 \equiv 3 \pmod{13}.$$