Math 406 Exam 1 Spring 2020 Solutions

1. Write down the prime factorization of 10!. [5 pts]

Solution: We have

\[10! = (10)(9)(8)(7)(6)(5)(4)(3)(2)(1) = (2 \cdot 5)(3^2)(2^3)(7)(2 \cdot 3)(5)(2^2)(3)(2) = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7.\]

2. Find the least nonnegative residue of 11^{67} \mod 13. [10 pts]

Solution: Since 11 \equiv -2 \mod 13 we have 11^2 \equiv 4 \mod 13, 11^4 \equiv 16 \equiv 3 \mod 13, 11^8 \equiv 9 \mod 13, 11^{16} \equiv 81 \equiv 3 \mod 13, 11^{32} \equiv 9 \mod 13, 11^{64} \equiv 3 \mod 13 and so 11^{67} \equiv 11^{64}11^211^1 \equiv (3)(4)(-2) \equiv 2 \mod 13.

3. Find all incongruent solutions mod 40, as least nonnegative residues, to the following linear congruence: [10 pts]

\[12x \equiv 28 \mod 40\]

Solution: Since gcd (12, 40) = 4 \mid 28 there are 4 incongruent solutions. One can be found by the EA or by noticing that 28 \equiv -12 \mod 40 so \(x \equiv -1\) is a solution. Then all solutions are then given by \(x \equiv -1 + k \left(\frac{40}{\gcd(40,12)}\right)\) \(\mod 40\) so this gives us \(x \equiv 39, 9, 19, 29 \mod 40\).

4. Use the Euclidean Algorithm to find gcd (390, 72) and write this as a linear combination of the two. [10 pts]

Solution: We have:

\[390 = 5(72) + 30\]
\[72 = 2(30) + 12\]
\[30 = 2(12) + 6\]
\[12 = 2(6) + 0\]

So gcd (390, 72) = 6 and we have:

\[6 = 30 - 2(12)\]
\[= 30 - 2(72 - 2(30))\]
\[= 5(30) - 2(72)\]
\[= 5(390 - 5(72)) - 2(72)\]
\[= 5(390) - 27(72)\]

5. Use the Chinese Remainder Theorem to find the smallest positive solution to the system: [15 pts]

\[x \equiv 2 \mod 5\]
\[x \equiv 1 \mod 6\]
\[x \equiv 4 \mod 7\]

Solution: We have \(M = (5)(6)(7) = 210, M_1 = (6)(7) = 42, M_2 = (5)(7) = 35\) and \(M_3 = (5)(6) = 30\). We then solve:

- \(42y_1 \equiv 1 \mod 5\) which is \(2y_1 \equiv 1 \mod 5\) which has solution \(y_1 \equiv 3 \mod 5\).
- \(35y_2 \equiv 1 \mod 6\) which is \(5y_2 \equiv 1 \mod 6\) which has solution \(y_2 \equiv 5 \mod 6\).
- \(30y_3 \equiv 1 \mod 7\) which is \(2y_3 \equiv 1 \mod 7\) which has solution \(y_3 \equiv 4 \mod 7\).

The solution is then \(x = (2)(42)(3) + (1)(35)(5) + (4)(30)(4) = 907 \equiv 67 \mod 210\).
6. Use mathematical induction to prove that:

\[ n! \geq n^3 \text{ for } n \geq 6 \]

**Solution:** For \( n = 6 \) we have \( 6! = 720 \) and \( 6^3 = 216 \) so the statement is true. Assume that for some \( k \geq 6 \) we have \( k! \geq k^3 \) and we claim that \( (k + 1)! \geq (k + 1)^3 \). This is equivalent to showing that \( k! \geq (k + 1)^2 \) which is equivalent to showing that \( k! - (k + 1)^2 \geq 0 \). Observe that:

\[
k! - (k + 1)^2 \geq k^3 - (k + 1)^2 = k^3 - k^2 - 2k - 1 = k(k^2 - k - 2) - 1 \geq 6(6(6 - 1) - 2) - 1 = 167 \geq 0
\]

7. One of the following two sets is well-ordered and one is not. Decide which is which and justify. \[ 15 \text{ pts} \]

You may assume only that \( \mathbb{Z}^+ \) is well-ordered.

\[
S_1 = [0, 1) \cap \mathbb{Q} \\
S_2 = \{1 - 2^k \mid k \in \mathbb{Z}^+\}
\]

**Solution:** The problem had an error: The set \( S_1 \) is not well-ordered because the subset \((0, 0) \cap \mathbb{Q}\) has no least element and the set \( S_2 \) is not well-ordered because the set itself has no least element.

8. Use the Fundamental Theorem of Arithmetic (uniqueness of prime factorization) to prove that \( \sqrt{2} \) is irrational. Hint: Use contradiction. \[ 10 \text{ pts} \]

**Solution:** Suppose \( \sqrt{2} = \frac{a}{b} \) with \( a, b \in \mathbb{Z}^+ \), then \( a^2 = 2b^2 \). If the PF of \( a \) is \( a = 2^\alpha A \) and if the PF of \( b \) is \( b = 2^\beta B \) then we have \( 2^{2\alpha} A^2 = 2^{2\beta+1} B^2 \) which is impossible since prime factorizations are unique.

9. Suppose \( a, b, c, d \in \mathbb{Z} \) with \( a \mid c \), \( b \mid c \), \( d = \gcd(a, b) \) and \( d^2 \mid c \). Prove that \( ab \mid c \). \[ 15 \text{ pts} \]

**Solution:** This problem had an error. For example if \( a = 2 \), \( b = 4 \) and \( c = 4 \) then \( a \mid c \) since \( 2 \mid 4 \), \( b \mid c \) since \( 4 \mid 4 \), \( d = \gcd(a, b) = 2 \) and \( d^2 \mid c \) since \( 4 \mid 4 \) but \( ab \nmid c \) since \( 8 \nmid 4 \).