Instructions. Answer each of the questions on your own paper, and be sure to show your work, including giving reasons, so that partial credit can be adequately assessed. Put your name on each page of your paper. There is a total possible of 80 points.

1. **[10 Points]**

   (a) Compute $\phi(1500)$.

   ▶ **Solution.** $1500 = 15 \cdot 100 = 3 \cdot 5 \cdot 2^2 \cdot 5^2 = 2^2 \cdot 3 \cdot 5^3$. Thus,

   $$\phi(1500) = (2^2 - 2)(3 - 1)(5^3 - 5^2) = 2 \cdot 2 \cdot 100 = \boxed{400}.$$

   ◀

   (b) Determine the remainder when 7^{1203} is divided by 1500. (*Hint:* Euler's Theorem.)

   ▶ **Solution.** Since $(7, 1500) = 1$, by Euler's theorem, $7^{\phi(1500)} \equiv 1 \pmod{1500}$ so $7^{400} \equiv 1 \pmod{1500}$. Hence,

   $$7^{1203} = 7^{3 \cdot 400 + 3} = (7^{400})^3 \cdot 7^3 \equiv 1^3 \cdot 7^3 \equiv 343 \pmod{1500}.$$

   Since the least residue of a modulo m is the remainder when a is divided by m, the remainder when 7^{1203} is divided by 1500 is $\boxed{343}$. ◀

2. **[12 Points]**

   (a) Give the definition of *congruence modulo* m. That is, complete the following sentence: Integers a and b are congruent modulo m (in notation $a \equiv b \pmod{m}$) if ... $m \mid (a - b)$ (or equivalently, $a = b + mk$ for some integer k).

   (b) Use the definition of congruence modulo m from part (a) to prove that if $a \equiv 3 \pmod{4}$ then $a^2 \equiv 1 \pmod{8}$.

   ▶ **Solution.** By assumption $1 \equiv 3 \pmod{4}$ so $a = 3 + 4k$ for some integer k. Then

   $$\begin{aligned} a^2 &= (3 + 4k)^2 \\ &= 9 + 24k + 16k^2 \\ &= 1 + 8 + 24k + 16k^2 \\ &= 1 + 8(1 + 3k + 2k^2) \\ &= 1 + 8s \quad \text{where } s = 1 + 3k + 2k^2 4 \text{ is an integer.} \end{aligned}$$

   Therefore, $a^2 - 1 = 8s$ where s is an integer and thus, $a^2 \equiv 1 \pmod{8}$ by the definition of congruence modulo 8. ◀

3. **[12 Points]** Use the Chinese Remainder Theorem to solve the following system of simultaneous congruences.

   $$\begin{aligned} x &\equiv 2 \pmod{5} \\ x &\equiv 4 \pmod{6} \\ x &\equiv -5 \pmod{7} \end{aligned}$$

▶ **Solution.** $c_1 = 2$, $m_1 = 5$, $M_1 = 42$, $42x_1 \equiv 1 \pmod 5$ so $2x_1 \equiv 1 \pmod 5$ and hence $x_2 \equiv 3 \pmod 5$.

$c_2 = 4$, $m_2 = 6$, $M_2 = 35$, $35x_2 \equiv 1 \pmod 6$ so $(-1)x_2 \equiv 1 \pmod 6$ and $x_2 \equiv -1 \pmod 6$.

$c_3 = -5$, $m_3 = 7$, $M_3 = 30$, $30x_3 \equiv 1 \pmod 7$ so $2x_3 \equiv 1 \pmod 7$ and $x_3 \equiv 4 \pmod 7$.

$M = 5 \cdot 6 \cdot 7 = 210$. Thus,

$$\begin{aligned} x &\equiv c_1M_1x_1 + c_2M_2x_2 + c_3M_3x_3 \pmod M \\ &\equiv 2 \cdot 42 \cdot 3 + 4 \cdot 35 \cdot (-1) + (-5) \cdot 30 \cdot 4 \pmod{210} \\ &\equiv -488 \pmod{210} \\ &\equiv 142 \pmod{210}. \end{aligned}$$

Check: $5 \mid (142 - 2)$, $6 \mid (142 - 4)$, $7 \mid (142 - (-5))$. ◀

4. **[14 Points]** Decide whether the following linear congruences are solvable. If so, give the least complete solution, if not say why there are no solutions.

   (a) $15x \equiv 17 \pmod{33}$.

   ▶ **Solution.** $(15, 33) = 3$ and $3 \nmid 17$ so there are no solutions. ◀

   (b) $21x \equiv 56 \pmod{91}$.

   ▶ **Solution.** $(21, 91) = 7$ and $7 \mid 56$ so there are 7 incongruent solutions modulo 91. To find one solution, divide the congruence by 7 to get $3x \equiv 8 \pmod{13}$. Since $13 - 4 \cdot 3 = 1$, $-4 \cdot 3 \equiv 1 \pmod{13}$ so multiplying by -4 gives $(-4) \cdot 3x \equiv (-4) \cdot 8 \pmod{13}$ so $x \equiv -32 \equiv 7 \pmod{13}$ is one solution to the original congruence. The other solutions are then $x_k = 7 + k\frac{91}{7}$ for $k = 0, 1, \ldots, 12$, so the least complete solution of the linear congruence is

   $$\{7, 20, 33, 46, 59, 72, 85\}.$$

   ◀

5. **[6 Points]** Let $f(x)$ be a polynomial with integer coefficients. Assume that $f(x) \equiv 0 \pmod 5$ has 4 solutions; $f(x) \equiv 0 \pmod 7$ has 5 solutions; $f(x) \equiv 0 \pmod 3$ has 2 solutions; and $f(x) \equiv 0 \pmod 4$ has no solutions. How many solutions does $f(x) \equiv 0 \pmod m$ have in each of the following cases:

   (a) $m = 21$; $5 \times 2 = 10$ solutions modulo 21.

   (b) $m = 28$; Any solution is also a solution modulo 4 and there are no solutions modulo 4, so there are no solutions modulo 28.

   (c) $m = 105$; $105 = 3 \cdot 5 \cdot 7$ so there are $2 \times 4 \times 5 = 40$ solutions modulo 105.

6. **[14 Points]**

   (a) Make a list of all the integers between 1 and 18 which are quadratic residues mod 19.

► **Solution.** The nonzero quadratic residues modulo 19 are the 9 squares modulo 19:

x	1	2	3	4	5	6	7	8	9
x^2	1	4	9	16	$25 \equiv 6$	$36 \equiv 17$	$49 \equiv 11$	$64 \equiv 7$	$81 \equiv 5$

That is, the set $\{1, 4, 5, 6, 7, 9, 11, 16, 17\}$. ◄

(b) Using your list in part (a), find a complete solution to the quadratic congruence

$$2x^2 + 2x + 7 \equiv 0 \pmod{19}.$$

► **Solution.** The discriminant is $b^2 - 4ac = 2^2 - 4 \cdot 2 \cdot 7 = -52 \equiv 5 \pmod{19}$, so from the table of squares we see that the equation $y^2 \equiv b^2 - 4ac \equiv 5 \pmod{19}$ has the solutions $y \equiv \pm 9 \pmod{19}$ or $y \equiv 9, 10 \pmod{19}$. Find the solution x of the quadratic by solving the linear congruence $2ax + b \equiv y \pmod{19}$ or

$$\begin{aligned} 4x + 2 &\equiv 9, 10 \pmod{19} \\ \implies 4x &\equiv 7, 8 \pmod{19}. \end{aligned}$$

Since $5 \cdot 4 = 20 \equiv 1 \pmod{19}$ we get that $x \equiv 5 \cdot 7, 5 \cdot 8 \pmod{19}$. That is, $x \equiv 16 \pmod{19}$ and $x \equiv 2 \pmod{19}$.

Alternate Solution: Since $7 \equiv -12 \pmod{19}$ the quadratic equivalence can be written as

$$2x^2 + 2x + 7 \equiv 0 \pmod{19} \implies 2x^2 + 2x - 12 \equiv 0 \pmod{19}.$$

This gives $2(x^2 + x - 6) \equiv 2(x + 3)(x - 2) \equiv 0 \pmod{19}$. This implies that there are solutions $x \equiv -3 \equiv 16 \pmod{19}$ and $x \equiv 2 \pmod{19}$. Since 19 is prime, Lagrange's theorem implies that these are the only solutions. ◄

7. **[12 Points]** Let $f(x) = x^3 + x^2 - 5$. Assuming that $x \equiv 2 \pmod{7}$ is the only solution to $f(x) \equiv 0 \pmod{7}$, find all solutions to $f(x) \equiv 0 \pmod{49}$.

► **Solution.** Since $x_1 \equiv 2 \pmod{7}$ is the only solution to $f(x) \equiv 0 \pmod{7}$, all solutions to $f(x) \equiv 0 \pmod{49}$ are of the form $x_2 = 2 + 7y$ where y is a solution of the linear congruence

$$\frac{f(x_1)}{7} + f'(x_1)y \equiv 0 \pmod{7}.$$

Since $f(2) = 8+4-5 = 7$ and $f'(x) = 3x^2+2x$ so $f'(2) = 16 \equiv 2 \pmod{7}$, y is a solution of the linear congruence $1 + 2y \equiv 0 \pmod{7}$ or $2y \equiv -1 \equiv 6 \pmod{7}$ which has the unique solution $y \equiv 3 \pmod{7}$ Thus, the unique solution of $f(x) \equiv 0 \pmod{49}$ is $x_2 = 2 + 7y = 2 + 7 \cdot 3 \equiv 23 \pmod{49}$. ◄