Department of Mathematics, University of Wisconsin-Madison

Math 467 — Exam 3 — Solutions — Fall 2023

NAME : (as it appears on Canvas)

EMAIL: @wisc.edu

PROFESSOR: MIKHAIL IVANOV

INSTRUCTIONS:

Time: **50 minutes**

Please write your name on every page.

No Calculators, No Notecards, No Notes

With the exception of the True/False question, you must justify your claims and use complete sentences in proofs.

You must use correct notation to receive full credit.

You can safely assume that all unknown quantitites in this exam, e.g. a, b, c, n, x, y, are always the integers.

Question:	1	2	3	4	5	6	Total
Points:	8	9	9	8	8	8	50

1. (8 points) For each statement below, CIRCLE true or false. You do not need to show your work.

   (a) $a^{10} \equiv 1 \pmod{11}$ for all values of a.
   False. Fails if $a = 0$.

   TRUE

   FALSE

   (b) The system of linear congruences

   $$\begin{cases} 3x + y \equiv 1 \pmod{5} \\ x + y \equiv 2 \pmod{5} \end{cases}$$

   has at least one solution.
   True because $3 \cdot 1 - 1 \cdot 1 = 2$ which is relatively prime to 5. Or just solve $x \equiv 2$, $y \equiv 0$.

   TRUE

   FALSE

   (c) The equation $3x \equiv 7 \pmod{9}$ has NO solutions.
   True, LHS is divisible by 3, by RHS not.

   TRUE

   FALSE

   (d) The equation $7x \equiv 3 \pmod{9}$ has NO solutions.
   False. $\gcd(7, 9) = 1$, so it is solvable.

   TRUE

   FALSE

First Name: ____________________ Last Name: ____________________

2. (9 points) **On this page, only the answer will be graded. MARK YOUR ANSWER CLEARLY. But you do not need to justify your work.**

   (a) Given that number $\overline{187x2}$ is divisible by 36, find the missing digit x.

   Since $9 \mid \overline{187x2}$ we know that $9 \mid 1+8+7+x+2 = 18+x$ and so $9 \mid x$ and so $x = 0$ or 9. Since $4 \mid \overline{187x2}$ we know that $4 \mid \overline{x2}$. And $4|92$ and does not divide $02 = 2$ so $\boxed{x = 9}$.

   (b) Compute $\tau(30)$.

   $\tau(30) = |\{1, 2, 3, 5, 6, 10, 15, 30\}| = \boxed{8}$.

   (c) Compute $\sigma(30)$.

   $\sigma(30) = 1 + 2 + 3 + 5 + 6 + 10 + 15 + 30 = \boxed{72}$.

3. (9 points) Find all primitive Pythagorean triples where $x = 24$. Show your work and write your answer clearly! You do not need to simplify any squares or products. E.g. if you come across something like $16^2 - 3^2$, then you do not need to simplify it.

We have $2st = 24$ so $st = 12$. The factorizations of 12 are $1 \cdot 12, 2 \cdot 6$ and $3 \cdot 4$. But $\gcd(2, 6) \neq 1$ so we only consider $(1, 12)$ and $(3, 4)$. These give the solutions:

$$(x, y, z) = (24, 12^2 - 1^1, 12^2 + 1^2) \text{ and } (24, 4^2 - 3^2, 4^2 + 3^2).$$

There is no need to simplify, but if you felt like simplifying, you'd get $(24, 143, 145)$ and $(24, 7, 25)$.

First Name: ______________________ Last Name: ______________________

4. (8 points) Solve

$$\begin{cases} 3x \equiv 4 \pmod{11} \\ x \equiv 2 \pmod{7} \end{cases}$$

Solution: Since $\gcd(3, 11) = 1$ and $\gcd(11, 7) = 1$, we know that this will have a solution.

We need to solve the first equation first:

$$3x \equiv 4 \pmod{11} \Leftrightarrow 12x \equiv 16 \pmod{11} \Leftrightarrow x \equiv 5 \pmod{11}$$

We can use the Euclidean algorithm to write $1 = a \cdot 11 + b \cdot 7$. This would yield $1 = 2 \cdot 11 + (-3) \cdot 7$.

So what we do is we take mix and match the RHS of the equations with these terms. Since it is $2 \pmod 7$ we put the 2 on the 11-term; and same with the 5. We get $2 \cdot 2 \cdot 11 + 5 \cdot (-3) \cdot 7$ and we claim that this will be our solution.

Let's check it with actual numbers. Our expression is $44 - 105 = -61 \equiv \boxed{16} \pmod{77}$. Modulo 11 we get $16 \equiv 5 \pmod{11}$ and $16 \equiv 2 \pmod 7$ and both are true.

Another Solution: We have $x \equiv 5 \pmod{11}$, so $x = 11k+5$, so $11k+5 \equiv 2 \pmod 7 \Rightarrow 11k \equiv 4 \pmod 7 \Rightarrow 4k \equiv 4 \pmod 7 \Rightarrow k \equiv 1 \pmod 7 \Rightarrow k = 7m + 1 \Rightarrow x = 11(7m + 1) + 5 = 77m + 16 \Rightarrow x \equiv 16 \pmod{77}$.

5. (8 points) If $\gcd(a, 35) = 1$ show that $a^{12} \equiv 1 \pmod{35}$.

Throughout we assume that $\gcd(a, 35) = 1$). We must show that $35 \mid (a^{12} - 1)$. Since $\gcd(5, 7) = 1$, it is equivalent to show that $7 \mid (a^{12} - 1)$ and $5 \mid (a^{12} - 1)$. Since $\gcd(a, 35) = 1$ it follows that neither 5 nor 7 divides a, and thus $\gcd(a, 5) = 1$ and $\gcd(a, 7) = 1$. By Fermat's Little Theorem for $p = 7$ we have $a^6 \equiv 1 \pmod 7$. Squaring both sides we get $a^{12} \equiv 1 \pmod 7$ and thus $7 \mid (a^{12} - 1)$. By Fermat's Little Theorem for $p = 5$ we have $a^4 \equiv 1 \pmod 5$. Cubing both sides we get $a^{12} \equiv 1 \pmod 5$ and thus $5 \mid (a^{12} - 1)$. Since $\gcd(5, 7) = 1$ we have that:

$$7 \mid (a^{12} - 1) \text{ and } 5 \mid (a^{12} - 1) \text{ and } \gcd(5, 7) = 1 \Rightarrow 21 \mid (a^{12} - 1)$$

which implies $a^{12} \equiv 1 \pmod{35}$ as desired.

6. (8 points) Find $10! \cdot 20!$ modulo 31.

$$\begin{aligned} 1 &\equiv -30 \pmod{31} \\ 2 &\equiv -29 \pmod{31} \\ 3 &\equiv -28 \pmod{31} \\ &\cdots \\ 10 &\equiv -21 \pmod{31} \end{aligned}$$

so

$$10! \equiv (-1)^{10} 21 \cdot 22 \cdot \ldots \cdot 30 \pmod{31},$$

and, but Wilson's Theorem

$$10! \cdot 20! \equiv 30! \equiv \boxed{\text{-1}} \pmod{31}.$$

Solution from a student: $-1 \equiv 30! = 20! \cdot 21 \cdot 22 \cdot 23 \cdot 24 \cdot 25 \cdot 26 \cdot 27 \cdot 28 \cdot 29 \cdot 30 \equiv 20! \cdot 7 \cdot 3 \cdot 2 \cdot 11 \cdot 23 \cdot 8 \cdot 3 \cdot 5 \cdot 5 \cdot 2 \cdot 13 \cdot 3 \cdot 9 \cdot 4 \cdot 7 \cdot 29 \cdot 2 \cdot 3 \cdot 5 \equiv 20! \cdot 10! \cdot 11 \cdot 23 \cdot 3 \cdot 13 \cdot 7 \cdot 29 \cdot 3 \cdot 5 \equiv 20! \cdot 10! \cdot 33 \cdot (-8) \cdot 39 \cdot 35 \cdot (-2) \equiv 20! \cdot 10! \cdot 2 \cdot 8 \cdot 8 \cdot 4 \cdot 2 \equiv 20! \cdot 10! \cdot 32^2 \cdot 20! \cdot 10!$.