1.3 Congruences

from **A Study Guide for Beginner's** by J.A.Beachy,
a supplement to **Abstract Algebra** by Beachy / Blair

29. Solve the congruence $42x \equiv 12 \pmod{90}$.

Comment: You need to recall Theorem 1.3.5, which states that $ax \equiv b \pmod{n}$ has a solution if an only if $\gcd(a, n)$ is a divisor of b. Also note that the congruence is stated modulo 90, and so the most satisfying answer is given in terms of congruence classes modulo 90.

Solution: We have $\gcd(42, 90) = 6$, so there is a solution since 6 is a factor of 12. Solving the congruence $42x \equiv 12 \pmod{90}$ is equivalent to solving the equation $42x = 12 + 90q$ for integers x and q. This reduces to $7x = 2 + 15q$, or $7x \equiv 2 \pmod{15}$. (Equivalently, we could obtain $7x \equiv 2 \pmod{15}$ by dividing $42x \equiv 12 \pmod{90}$ through by 6.) We next use trial and error to look for the multiplicative inverse of 7 modulo 15. The numbers congruent to 1 modulo 15 are 16, 31, 46, 61, etc., and -14, -29, -44, etc. Among these, we see that 7 is a factor of -14, so we multiply both sides of the congruence by -2 since $(-2)(7) = -14 \equiv 1 \pmod{15}$. Thus we have $-14x \equiv -4 \pmod{15}$, or $x \equiv 11 \pmod{15}$. The solution is $x \equiv 11, 26, 41, 56, 71, 86 \pmod{90}$.

30. (a) Find all solutions to the congruence $55x \equiv 35 \pmod{75}$.

Solution: We have $\gcd(55, 75) = 5$, which is a divisor of 35. Thus we have

$55x \equiv 35 \pmod{75}$; $11x \equiv 7 \pmod{15}$; $44x \equiv 28 \pmod{15}$;

$-x \equiv 13 \pmod{15}$; $x \equiv 2 \pmod{15}$. The solution is

$x \equiv 2, 17, 32, 47, 62 \pmod{75}$.

Comment: In the solution, the congruence $11x \equiv 7 \pmod{15}$ is multiplied by 4 since trial and error produces the congruence $4 \cdot 11 \equiv -1 \pmod{15}$, a relatively easy way to eliminate the coefficient of x.

(b) Find all solutions to the congruence $55x \equiv 36 \pmod{75}$.

Solution: There is no solution, since $\gcd(55, 75) = 5$ is not a divisor of 36.

31. (a) Find one particular integer solution to the equation $110x + 75y = 45$.

Solution: By Theorem 1.1.6, any linear combination of 110 and 75 is a multiple of their greatest common divisor. We have following matrix reduction.

$$\begin{bmatrix} 1 & 0 & 110 \\ 0 & 1 & 75 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 35 \\ 0 & 1 & 75 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 35 \\ -2 & 3 & 5 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 15 & -22 & 0 \\ -2 & 3 & 5 \end{bmatrix}$$

Thus $-2(110) + 3(75) = 5$, and multiplying by 9 yields a solution: $x = -18$, $y = 27$, since $110(-18) + 75(27) = 45$.

Alternate solution: The equation reduces to the congruence $35x \equiv 45 \pmod{75}$. This simplifies to $7x \equiv 9 \pmod{15}$, and multiplying both sides by -2 gives $x \equiv -3 \pmod{15}$. Thus $75y = 45 + 3(110) = 375$ and so $x = -3$, $y = 5$ is a solution.

Comment: The matrix computation (above) shows that $110(15) + 75(-22) = 0$, so adding any multiple of the vector $(15, -22)$ to the particular solution $(-18, 27)$ must also give you a solution. That is the motivation for part (b) of the problem.

(b) Show that if $x = m$ and $y = n$ is an integer solution to the equation in part (a), then so is $x = m + 15q$ and $y = n - 22q$, for any integer q.

Solution: If $110m + 75n = 45$, then $110(m + 15q) + 75(n - 22q) = 45 + 110(15)q + 75(-22)q = 45$, since $110(15) - 75(22) = 0$.

32. Solve the system of congruences $\quad x \equiv 2 \pmod 9 \quad x \equiv 4 \pmod{10}$.

Solution: We can easily find a linear combination of 9 and 10 that equals 1, by just writing $(1)(10) + (-1)(9) = 1$. Using the method outlined in the proof of Theorem 1.3.6, the solution is $x \equiv (2)(1)(10) + (4)(-1)(9) = -16 \pmod{90}$.

Alternate solution: Convert the second congruence to the equation $x = 4 + 10q$ for some $q \in \mathbf{Z}$, and substitute for x in the second congruence. Then $4+10q \equiv 2 \pmod 9$, which reduces to $q \equiv 7 \pmod 9$. The solution is $x \equiv 4 + 10(7) \equiv 74 \pmod{90}$.

33. Solve the system of congruences $\quad x \equiv 5 \pmod{25} \quad x \equiv 23 \pmod{32}$.

Solution: To solve $r(32) + s(25) = 1$ we will use the matrix method. $\begin{bmatrix} 1 & 0 & 32 \\ 0 & 1 & 25 \end{bmatrix} \rightsquigarrow$ $\begin{bmatrix} 1 & -1 & 7 \\ 0 & 1 & 25 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 1 & -1 & 7 \\ -3 & 4 & 4 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 4 & -5 & 3 \\ -3 & 4 & 4 \end{bmatrix} \rightsquigarrow \begin{bmatrix} 4 & -5 & 3 \\ -7 & 9 & 1 \end{bmatrix}$ Thus $(-7)(32) + (9)(25) = 1$, and so $x \equiv (5)(-7)(32) + (23)(9)(25) = 4025 \equiv 55 \pmod{800}$.

Alternate solution: Write $x = 23+32q$ for some $q \in \mathbf{Z}$, and substitute to get $23+32q \equiv 5 \pmod{25}$, which reduces to $7q \equiv 7 \pmod{25}$, so $q \equiv 1 \pmod{25}$. This gives $x \equiv 55 \pmod{800}$.

34. Solve the system of congruences $\quad 5x \equiv 14 \pmod{17} \quad 3x \equiv 2 \pmod{13}$.

Solution: By trial and error, $7 \cdot 5 \equiv 1 \pmod{17}$ and $9 \cdot 3 \equiv 1 \pmod{13}$,

so $5x \equiv 14 \pmod{17}$; $\quad 35x \equiv 98 \pmod{17}$; $\quad x \equiv 13 \pmod{17}$

and $3x \equiv 2 \pmod{13}$; $\quad 27x \equiv 18 \pmod{13}$; $\quad x \equiv 5 \pmod{13}$.

Having reduced the system to the standard form, we can solve it in the usual way. We have $x = 13 + 17q$ for some $q \in \mathbf{Z}$, and then $13 + 17q \equiv 5 \pmod{13}$. This reduces to $4q \equiv 5 \pmod{13}$, so $40q \equiv 50 \pmod{13}$, or $q \equiv 11 \pmod{13}$. This leads to the answer, $x \equiv 13 + 17 \cdot 11 \equiv 200 \pmod{221}$.

35. Give integers a, b, m, n to provide an example of a system

$$x \equiv a \pmod m \qquad x \equiv b \pmod n$$

that has no solution.

Solution: In the example the integers m and n cannot be relatively prime. This is the clue to take $m = n = 2$, with $a = 1$ and $b = 0$.

36. Find the additive order of each of the following integers, module 20: 4, 5, 6, 7, and 8.

Note: The additive order of a modulo n is defined to be the smallest positive solution of the congruence $ax \equiv 0 \pmod{n}$.

Solution: To find the additive order of 4, we need to solve the congruence $4x \equiv 0 \pmod{20}$. Dividing each term by $\gcd(4, 20) = 4$, we obtain $x \equiv 0 \pmod{5}$, and then the smallest positive solution is $x = 5$. Thus 4 has additive order 5 modulo 20.

The additive order of 5 modulo 20 is 4, as shown by this solution of $4x \equiv 0 \pmod{20}$.

$5x \equiv 0 \pmod{20}$ $\quad x \equiv 0 \pmod{4}$ $\quad x = 4.$

The additive order of 6 modulo 20 is 10:

$6x \equiv 0 \pmod{20}$ $\quad 3x \equiv 0 \pmod{10}$ $\quad x \equiv 0 \pmod{10}$ $\quad x = 10.$

The additive order of 7 modulo 20 is 20:

$7x \equiv 0 \pmod{20}$ $\quad x \equiv 0 \pmod{20}$ $\quad x = 20.$

The additive order of 8 modulo 20 is 5:

$8x \equiv 0 \pmod{20}$ $\quad 2x \equiv 0 \pmod{5}$ $\quad x \equiv 0 \pmod{5}$ $\quad x = 5.$

37. (a) Compute the last digit in the decimal expansion of 4^{100}.

Solution: The last digit is the remainder when divided by 10. Thus we must compute the congruence class of $4^{100} \pmod{10}$. We have $4^2 \equiv 6 \pmod{10}$, and then $6^2 \equiv 6 \pmod{10}$. This shows that $4^{100} = (4^2)^{50} \equiv 6^{50} \equiv 6 \pmod{10}$, so the units digit of 4^{100} is 6.

(b) Is 4^{100} divisible by 3?

Solution: No, since $4^{100} \equiv 1^{100} \equiv 1 \pmod{3}$. Or you can write 2^{200} as the prime factorization, and then $\gcd(3, 2^{200}) = 1$.

38. Find all integers n for which $13 \mid 4(n^2 + 1)$.

Solution: This is equivalent to solving the congruence $4(n^2 + 1) \equiv 0 \pmod{13}$. Since $\gcd(4, 13) = 1$, we can cancel 4, to get $n^2 \equiv -1 \pmod{13}$. Just computing the squares modulo 13 gives us $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 \equiv 3 \pmod{13}$, $(\pm 5)^2 \equiv -1 \pmod{13}$, and $(\pm 6)^2 \equiv -3 \pmod{13}$. We have done the computation for representatives of each congruence class, so the answer to the original question is $n \equiv \pm 5 \pmod{13}$. *Comment:* For example, if $n = 5$, then $13 \mid 4 \cdot 26$.

39. Prove that $10^{n+1} + 4 \cdot 10^n + 4$ is divisible by 9, for all positive integers n.

Comment: This could be proved by induction, but we can give a more elegant proof using congruences.

Solution: The proof consists of simply observing that $10^{n+1} + 4 \cdot 10^n + 4 \equiv 0 \pmod{9}$ since $10 \equiv 1 \pmod{9}$.

40. Prove that for any integer n, the number $n^3 + 5n$ is divisible by 6.

Solution: By Proposition 1.2.3 (c), it is enough to show that $n^3 + 5n \equiv 0 \pmod{2}$ and $n^3 + 5n \equiv 0 \pmod{3}$, reducing the question to just a few computations. Modulo

2, we have $0^3 + 5(0) \equiv 0 \pmod 2$, and $1^3 + 5(1) = 6 \equiv 0 \pmod 2$. Modulo 3, we have $0^3 + 5(0) \equiv 0 \pmod 3$, $1^3 + 5(1) = 6 \equiv 0 \pmod 3$, and $2^3 + 5(2) \equiv 8 + 10 \equiv 0 \pmod 3$. Therefore $6 \mid n^3 + 5n$.

41. Use techniques of this section to prove that if m and n are odd integers, then $m^2 - n^2$ is divisible by 8. (Compare Problem 1.2.36.)

Solution: We need to show that if m and n are odd, then $m^2 - n^2 \equiv 0 \pmod 8$. Modulo 8, any odd integer is congruent to either ± 1 or ± 3, and squaring any of these four values gives 1 (mod 8). Thus $m^2 - n^2 \equiv 1 - 1 \equiv 0 \pmod 8$.

42. Prove that $4^{2n+1} - 7^{4n-2}$ is divisible by 15, for all positive integers n.

Solution: We have $4^2 \equiv 1 \pmod{15}$, so $4^{2n+1} = (4^2)^n \cdot 4 \equiv 4 \pmod{15}$. We also have $7^2 \equiv 4 \pmod{15}$, so $7^4 \equiv 1 \pmod{15}$, and thus $7^{4n-2} \equiv 7^2 \cdot (7^4)^{n-1} \equiv 4 \pmod{15}$. Therefore $4^{2n+1} - 7^{4n-2} \equiv 4 - 4 \equiv 0 \pmod{15}$.

Alternate solution: By Proposition 1.2.3 (c), it is enough to show that $4^{2n+1} - 7^{4n-2} \equiv 0 \pmod 3$ and $4^{2n+1} - 7^{4n-2} \equiv 0 \pmod 5$. We have $4^{2n+1} - 7^{4n-2} \equiv 1^{2n+1} - 1^{4n-2} \equiv 1 - 1 \equiv 0 \pmod 3$ and $4^{2n+1} - 7^{4n-2} \equiv (-1)^{2n+1} - 2^{2(2n-1)} \equiv (-1)^{2n+1} - (2^2)^{2n-1} \equiv (-1)^{2n+1} - (-1)^{2n-1} \equiv -1 - (-1) \equiv 0 \pmod 5$.

43. Prove that the fourth power of an integer can only have 0, 1, 5, or 6 as its units digit.

Solution: Since the question deals with the units digit of n^4, it is really asking to find $n^4 \pmod{10}$. All we need to do is to compute the fourth power of each congruence class modulo 10: $0^4 = 0$, $(\pm 1)^4 = 1$, $(\pm 2)^4 = 16 \equiv 6 \pmod{10}$, $(\pm 3)^4 = 81 \equiv 1 \pmod{10}$, $(\pm 4)^4 \equiv 6^2 \equiv 6 \pmod{10}$, and $5^4 \equiv 5^2 \equiv 5 \pmod{10}$. This shows that the only possible units digits for n^4 are 0, 1, 5, and 6.

ANSWERS AND HINTS

45. Solve the following congruences.
(a) $10x \equiv 5 \pmod{21}$ *Answer:* $x \equiv 11 \pmod{21}$
(b) $10x \equiv 5 \pmod{15}$ *Answer:* $x \equiv 2, 5, 8, 11, 14 \pmod{15}$
(c) $10x \equiv 4 \pmod{15}$ *Answer:* No solution
(d) $10x \equiv 4 \pmod{14}$ *Answer:* $x \equiv 6, 13 \pmod{14}$

47. Solve the following congruence. $20x \equiv 12 \pmod{72}$
Answer: $x \equiv 15, 33, 51, 69 \pmod{72}$

49. (a) Find the additive order of each of the following elements, by solving the appropriate congruences. 4, 5, 6 modulo 24
Answer: The congruence class of 4 has additive order 6, that of 5 has additive order 24, and that of 6 has additive order 4 (modulo 24).

53. Solve the following system of congruences: $x \equiv 11 \pmod{16}$ $x \equiv 18 \pmod{25}$
Answer: $x \equiv 43 \pmod{400}$

55. Solve the following system of congruences: $x \equiv 9 \pmod{25}$ $x \equiv 13 \pmod{18}$
Answer: $x \equiv -41 \equiv 409 \pmod{450}$

57. Solve this system: $2x \equiv 3 \pmod 7$ $x \equiv 4 \pmod 6$ $5x \equiv 50 \pmod{55}$
Answer: $x \equiv 208 \pmod{462}$

59. Use congruences to prove that $5^{2n} - 1$ is divisible by 24, for all positive integers n.
Solution: We have $5^{2n} = (5^2)^n \equiv 1^n \equiv 1 \pmod{24}$.

61. Prove that if $0 < n < m$, then $2^{2^n} + 1$ and $2^{2^m} + 1$ are relatively prime.
Hint: Write 2^{2^m} as a power of 2^{2^n}. If p is a common prime divisor, reduce modulo p.