MATH 135 Algebra, Solutions to Assignment 9

1: Solve the following pairs of congruences.

(a) $x \equiv 5 \pmod 7$
$x \equiv 8 \pmod{15}$

Solution: We have $x \equiv 5 \pmod 7$ when $x \in \{\cdots, -2, 5, 12, 19, 26, 33, 40, 47, 54, 61, 68, \cdots\}$, and we have $x \equiv 8 \pmod{15}$ when $x \in \{\cdots, -7, 8, 23, 38, 53, 68, \cdots\}$. Thus one solution is $x = 68$ and so, by the Chinese Remainder Theorem, the general solution is $x \equiv 68 \pmod{105}$.

(b) $x \equiv 45 \pmod{84}$
$x \equiv 61 \pmod{115}$

Solution: For x to be a solution, we need $x = 45 + 84r$ and $x = 61 + 115s$ for some integers r and s, so we need $45 + 8r = 61 + 115s$, that is $84r - 115s = 16$. The Euclidean Algorithm gives

$$115 = 1 \cdot 84 + 31\ , \quad 84 = 2 \cdot 31 + 22\ , \quad 31 = 1 \cdot 22 + 9\ , \quad 22 = 2 \cdot 9 + 4\ , \quad 9 = 2 \cdot 4 + 1$$

so we have $\gcd(84, 115) = 1$, and the Back-Substitution gives

$$1\ , \quad -2\ , \quad 5\ , \quad -7\ , \quad 19\ , \quad -26$$

and so we have $(84)(-26) - (115)(-19) = 1$. Multiply both sides by 16 to get $(84)(-416) - (115)(-304) = 16$. Thus one solution to the equation $84r - 115s = 16$ is given by $(r, s) = (-416, -304)$, and by the Linear Diophantine Equation Theorem, the general solution is $(r, s) = (-416, -304) + k(115, 84)$, $k \in \mathbf{Z}$, so we have $r \equiv -416 \equiv 44 \pmod{115}$. Thus one solution to the given pair of congruences is $x = 45 + 84r = 45 + 84 \cdot 44 = 3741$. Note that $84 \cdot 115 = 9660$, so by the Chinese Remainder Theorem, the general solution to the given pair of congruences is

$$x \equiv 3741 \pmod{9660}\,.$$

2: Solve the following pairs of congruences.

(a) $15x \equiv 4 \pmod{26}$

$24x \equiv 6 \pmod{63}$

Solution: First we solve the linear congruence $15x = 4 \pmod{26}$. By inspection, one solution is $x = 2$ and we have $\gcd(15, 26) = 1$, and so by the Linear Congruence Theorem, the general solution is $x \equiv 2 \pmod{26}$. Next we solve $24x \equiv 6 \pmod{63}$. We need $24x + 63y = 6$. The Euclidean Algorithm gives

$$63 = 2 \cdot 24 + 15\ ,\quad 24 = 1 \cdot 15 + 9\ ,\quad 15 = 1 \cdot 9 + 6\ ,\quad 9 = 1 \cdot 6 + 3\ ,\quad 6 = 2 \cdot 3 + 0$$

so we have $\gcd(24, 63) = 3$, and then Back-Substitution gives

$$1\ ,\quad -1\ ,\quad 2\ ,\quad -3\ ,\quad 8$$

so we have $(24)(8) + (63)(-3) = 3$. Multiply both sides by 2 to get $(24)(16) + (63)(-6) = 6$. Thus one solution is $x = 16$. Note that $\frac{63}{3} = 21$, so by the Linear Congruence Theorem, the general solution to the congruence $24x \equiv 6 \pmod{63}$ is $x \equiv 16 \pmod{21}$. Thus the original pair of congruences is equivalent to the pair of congruences

$$\begin{aligned} x &\equiv 2 \pmod{26} \\ x &\equiv 16 \pmod{21} \end{aligned}\ .$$

For x to be a solution we need $x = 2 + 26r$ and $x = 16 + 21s$ for some integers r and s, so we must have $2 + 26r = 16 + 21s$, that is $26r - 21s = 14$. The Euclidean Algorithm gives $26 = 1 \cdot 21 + 5$, $21 = 4 \cdot 5 + 1$ so we have $\gcd(26, 21) = 1$, and then Back-Substitution gives 1, -4, 5, so we have $(26)(-4) - (21)(-5) = 1$. Multiply both sides by 14 to get $(26)(-56) - (21)(-70) = 14$. Thus one solution is $(r, s) = (-56, -70)$ and the general solution is $(r, s) = (-56, -70) + k(21, 26)$, $k \in \mathbf{Z}$, so we have $r \equiv -56 \equiv 7 \pmod{21}$. Thus one solution to the pair of congruences is $x = 2 + 26r = 2 + 26 \cdot 7 = 184$, and by the Chinese Remainder Theorem, the general solution is

$$x \equiv 184 \pmod{546}\,.$$

(b) $2x^3 \equiv 7 \pmod{9}$

$x^2 \equiv x + 6 \pmod{35}$

Solution: First we solve the congruence $2x^3 \equiv 7 \pmod{9}$ by making a table of values modulo 9.

x	0	1	2	3	4	5	6	7	8
x^2	0	1	4	0	7	7	0	4	1
x^3	0	1	8	0	1	8	0	1	8
$2x^3$	0	2	7	0	2	7	0	2	7

From the table, we see that $2x^3 \equiv 7 \pmod{9}$ when $x \equiv 2 \pmod{3}$.

Next we solve the congruence $x^2 \equiv x + 6 \pmod{35}$. By the Chinese Remainder Theorem, x satisfies this single congruence if and only if x satisfies the pair of congruences $x^2 \equiv x + 6 \pmod{5}$ and $x^2 \equiv x + 6 \pmod{7}$. We make a table of values modulo 5 and a table of values modulo 7.

x	0	1	2	3	4
x^2	0	1	4	4	1
$x + 6$	1	2	3	4	0

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1
$x + 6$	6	0	1	2	3	4	5

From the first table we see that $x^2 \equiv x + 6 \pmod{5}$ when $x = 3 \pmod{5}$, and from the second table we see that $x^2 \equiv x + 6 \pmod{7}$ when $x = 3$ or $5 \pmod{7}$. By the Chinese Remainder Theorem, we have $x \equiv 3 \pmod{5}$ and $x \equiv 3 \pmod{7}$ when $x \equiv 3 \pmod{35}$. Also, note that $x = -2$ is one solution to $x \equiv 3 \pmod{5}$ and $x \equiv 5 \pmod{7}$, so by the Chinese Remainder Theorem, the general solution to this pair of congruences is $x \equiv -2 \equiv 33 \pmod{35}$. Thus we have shown that $x^2 \equiv x + 6 \pmod{35}$ when $x \equiv 3$ or $33 \pmod{35}$.

We have shown that the original pair of congruences is equivalent to

$$x \equiv 2 \pmod{3} \quad \text{and} \quad x \equiv 3 \text{ or } 33 \pmod{35}\,.$$

Note that $x = 38$ is one solution to the pair of congruences $x \equiv 2 \pmod{3}$ and $x \equiv 3 \pmod{33}$, so by the Chines Remainder Theorem, the general solution to this pair is $x \equiv 38 \pmod{105}$. Also, note that $x = 68$ is one solution to the pair of congruences $x \equiv 2 \pmod{3}$ and $x \equiv 33 \pmod{35}$, and so by the Chinese Remainder Theorem, the general solution to this pair is $x \equiv 68 \pmod{105}$. Thus the complete solution to the original pair of congruences is

$$x \equiv 38 \text{ or } 68 \pmod{105}\,.$$

3: Chinese generals used to count their troops by telling them to form groups of some size n, and then counting the number of troops left over. Suppose there were 5000 troops before a battle, and after the battle it was found that when the troops formed groups of 5 there was 1 left over, when they formed groups of 7 there were none left over, when they formed groups of 11 there were 6 left over, and when they formed groups of 12 there were 5 left over. How many troops survived the battle?

Solution: We must solve the system of congruences

$$\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 0 \pmod{7} \\ x &\equiv 6 \pmod{11} \\ x &\equiv 5 \pmod{12}\,. \end{aligned}$$

Note that $x = 21$ is a solution to the first pair of congruences so by the Chinese Remainder Theorem, the general solution to the first pair is $x \equiv 21 \pmod{35}$. Also note that $x = 17$ is a solution to the second pair of congruences, so the general solution is $x \equiv 17 \pmod{132}$. Thus we must solve the pair of congruences

$$\begin{aligned} x &\equiv 21 \pmod{35} \\ x &\equiv 17 \pmod{132}\,. \end{aligned}$$

For x to be a solution we need $x = 21 + 35r$ and $x = 17 + 132s$ for some integers r and s, so we must have $21 + 35r = 17 + 132s$, that is $35r - 132s = -4$. The Euclidean Algorithm gives

$$132 = 3 \cdot 35 + 27\,, \quad 35 = 1 \cdot 27 + 8\,, \quad 27 = 3 \cdot 8 + 3\,, \quad 8 = 2 \cdot 3 + 2\,, \quad 3 = 1 \cdot 2 + 1$$

so we have $\gcd(35, 132) = 1$, and then Back-Substitution gives

$$1\,, \quad -1\,, \quad 3\,, \quad -10\,, \quad 13\,, \quad -49$$

and so we have $(35)(-49) - (132)(-13) = 1$. Multiply both sides by -4 to get $(35)(196) - (132)(52) = -4$. Thus one solution to the linear diophantine equation $35r - 132s = -4$ is given by $(r, s) = (196, 52)$, and by the Linear Diophantine Equation Theorem, the general solution is $(r, s) = (196, 52) + k(132, 35)$, $k \in \mathbf{Z}$, so we have $r \equiv 196 \equiv 64 \pmod{132}$. Thus one solution to the above pair of congruences is $x = 21 + 35r = 21 + (35)(64) = 2261$. Note that $35 \cdot 132 = 4620$, so by the Chinese Remainder Theorem, the general solution to the pair of congruneces is

$$x \equiv 2261 \pmod{4620}\,.$$

Since $2261 - 4620 < 0$ and $2261 + 4620 > 5000$, there must be 2261 troops remaining after the battle.

4: (a) Find $\phi(n)$ for all integers n with $20 \le n \le 30$.

Solution: We have

$$\begin{aligned}
&\phi(20) = \phi(2^2 \cdot 5) = \phi(2^2)\phi(5) = 2^1(2-1) \cdot 4 = 8\\
&\phi(21) = \phi(3 \cdot 7) = \phi(3)\phi(7) = 2 \cdot 6 = 12\\
&\phi(22) = \phi(2 \cdot 11) = \phi(2)\phi(11) = 1 \cdot 10 = 10\\
&\phi(23) = 22\\
&\phi(24) = \phi(2^3 \cdot 3) = \phi(2^3)\phi(3) = 2^2(2-1) \cdot 2 = 8\\
&\phi(25) = \phi(5^2) = 5^1(5-1) = 20\\
&\phi(26) = \phi(2 \cdot 13) = \phi(2)\phi(13) = 1 \cdot 12 = 12\\
&\phi(27) = \phi(3^3) = 3^2(3-1) = 18\\
&\phi(28) = \phi(2^2 \cdot 7) = \phi(2^2)\phi(7) = 2^1(2-1) \cdot 6 = 12\\
&\phi(29) = 28\\
&\phi(30) = \phi(2 \cdot 3 \cdot 5) = \phi(2)\phi(3)\phi(5) = 1 \cdot 2 \cdot 4 = 8\,.
\end{aligned}$$

(b) Find all positive integers n such that $\phi(n) = 60$.

Solution: We begin by finding $\phi(p^k)$ for all prime powers p^k for which $\phi(p^k) \le 60$, and we list those for which $\phi(p^k) \big| 60$:

$\phi(2) = 1$ $\phi(3) = 2$ $\phi(5) = 4$ $\phi(7) = 6$ $\phi(11) = 10$ $\phi(13) = 12$ $\phi(31) = 30$ $\phi(61) = 60$
$\phi(4) = 2$ $\phi(9) = 6$ $\phi(25) = 20$
$\phi(8) = 4$

Note that except for $\phi(2)$, these are all even, and the only ways to factor 60 into two even integers are $60 = 2 \cdot 30$ and $60 = 6 \cdot 10$. When n has exactly one prime factor, say $n = p^k$, so that we have $60 = \phi(n) = \phi(p^k)$, we must have $n = p^k = 61$. When n has exactly two prime factors, say $n = p^k q^l$ with $\phi(p^k) \le \phi(q^l)$, so that $60 = \phi(n) = \phi(p^k)\phi(q^l)$, we must have one of the following situations:

$$\begin{aligned}
&\phi(p^k) = 1 \text{ and } \phi(q^l) = 60 \text{ , in which case } p^k = 2 \text{ and } q^l = 61\\
&\phi(p^k) = 2 \text{ and } \phi(q^l) = 30 \text{ , in which case } p^k = 2^2 \text{ or } 3 \text{ and } q^l = 31\\
&\phi(p^k) = 6 \text{ and } \phi(q^l) = 10 \text{ , in which case } p^k = 3^2 \text{ or } 7 \text{ and } q^l = 11\,.
\end{aligned}$$

When n has exactly three prime factors, say $n = p^k q^l r^m$ with $\phi(p^k) \le \phi(q^l) \le \phi(r^m)$, so that we have $60 = \phi(n) = \phi(p^k)\phi(q^l)\phi(r^m)$, we must have one of the following:

$$\begin{aligned}
&\phi(p^k) = 1, \phi(q^l) = 2 \text{ and } \phi(r^m) = 30 \text{ , in which case } p^k = 2, q^l = 3 \text{ and } r^m = 31\\
&\phi(p^k) = 1, \phi(q^l) = 6 \text{ and } \phi(r^m) = 10 \text{ , in which case } p^k = 2, q^l = 3^2 \text{ or } 7 \text{ and } r^m = 11\,.
\end{aligned}$$

Thus the possible values of n are

$$61\,,\quad 2 \cdot 61\,,\quad 2^2 \cdot 31\,,\quad 3 \cdot 31\,,\quad 3^2 \cdot 11\,,\quad 7 \cdot 11\,,\quad 2 \cdot 3 \cdot 31\,,\quad 2 \cdot 3^2 \cdot 11\,,\quad 2 \cdot 7 \cdot 11\,.$$

From smallest to largest, the possible values for n are 61, 77, 93, 99, 122, 124, 154, 186 and 198.

5: (a) Show that $2^{340} \equiv 1 \pmod{341}$.

Solution: Note that $341 = 11 \cdot 31$. By Fermat's Little Theorem, we have $2^{10} \equiv 1 \pmod{11}$ and so we have $2^{340} \equiv (2^{10})^{34} \equiv 1^{34} \equiv 1 \pmod{11}$. Also, notice that $2^5 = 32 \equiv 1 \pmod{31}$, and so we have $2^{340} \equiv (2^5)^{68} \equiv 1^{68} \equiv 1 \pmod{31}$. Thus by the Chinese Remainder Theorem, $2^{340} \equiv 1 \pmod{341}$.
(We remark that this gives a counterexample to the conjecture we made in our solution to Problem 4(b) of Assignment 1).

(b) Show that $21 \big| (4n^7 + 7n^3 + 10n)$ for all integers n.

Solution: Note that $21 = 3 \cdot 7$, so we shall work modulo 3 and modulo 7. By Fermat's Little Theorem, we have $n^7 \equiv n^5 \equiv n^3 \equiv n \pmod{3}$ for all n, and so

$$4n^7 + 7n^3 + 10n \equiv 4n + 7n + 10n \equiv 21n \equiv 0 \pmod{3}\,.$$

Also, by Fermat's Little Theorem again, we have $n^7 \equiv n \pmod{7}$ for all n and so

$$4n^7 + 7n^3 + 10n \equiv 4n + 7n^3 + 10n \equiv 7n^3 + 14n \equiv 0 \pmod{7}\,.$$

By the Chinese Remainder Theorem, we have $4n^7 + 7n^3 + 10n \equiv 0 \pmod{21}$, that is $21 \big| (4n^7 + 7n^3 + 10n)$, for all integers n.

(c) Find a positive integer k such that the number 3^k ends with the digits 0001.

Solution: By the Euler Fermat Theorem, we have $3^{\phi(10000)} \equiv 1 \pmod{10000}$, that is $3^{\phi(10000)} = 1 + 10000l$ for some integer l. Thus $3^{\phi(10000)}$ ends with the digits 0001, so we can take

$$k = \phi(10000) = \phi(2^4)\phi(5^4) = 2^3(2-1) \cdot 5^3(5-1) = 8 \cdot 500 = 4000\,.$$

(In fact we can take k to be any multiple of 500 because we have $3^4 \equiv 81 \equiv 1 \pmod{2^4}$ which implies that $3^{500} = (3^4)^{125} = 1^{125} \equiv 1 \pmod{2^4}$, and we have $3^{500} \equiv 3^{\phi(5^4)} \equiv 1 \pmod{5^4}$).

(d) Let $n = p^k$ for some positive integer k where p is prime with $p \equiv 3 \pmod{4}$. Show that the congruence $x^2 \equiv -1 \pmod{n}$ has no solution.

Solution: Since $p \equiv 3 \pmod{4}$ we have $(p-1) \equiv 2 \pmod{4}$ and we have $p^{k-1} \equiv 1$ or $3 \pmod{4}$ (1 if k is odd and 3 if k is even), and so $\phi(n) = \phi(p^k) = p^{k-1}(p-1) \equiv 2 \pmod{4}$. Thus $\phi(n) = 2 + 4l$ for some integer l, so $\phi(n)/2 = 1 + 2l$, which is an odd number. If we had $x^2 \equiv -1 \pmod{n}$ then we would have $x^{\phi(n)} \equiv (x^2)^{\phi(n)/2} \equiv (-1)^{\phi(n)/2} \equiv -1 \pmod{n}$, which would contradict the Euler Fermat Theorem.