Chapter 4.4: Systems of Congruences
Friday, July 10

Linear congruences
Find all solutions:

1. $7n \equiv 1 \pmod{19}$

\[
\begin{align*}
19 - 2 \cdot 7 &= 5 \\
7 - 5 &= 2 \\
5 - 2 \cdot 2 &= 1 \\
5 - 2 \cdot (7 - 5) &= 1 \\
3 \cdot 5 - 2 \cdot 7 &= 1 \\
3 \cdot (19 - 2 \cdot 7) - 2 \cdot 7 &= 1 \\
3 \cdot 19 - 8 \cdot 7 &= 1 \\
-8 \cdot 7 &= 1 \pmod{19} \\
11 \cdot 7 &= 1 \pmod{19}
\end{align*}
\]

2. $8n \equiv 3 \pmod{23}$

\[
\begin{align*}
23 - 2 \cdot 8 &= 7 \\
8 - 7 &= 1 \\
8 - (23 - 2 \cdot 8) &= 1 \\
3 \cdot 8 - 23 &= 1 \\
3 \cdot 8 &\equiv 1 \pmod{23} \\
9 \cdot 8 &\equiv 3 \pmod{23}
\end{align*}
\]

3. $5n \equiv 6 \pmod{11}$

Try this with some trial and error:

\[
\begin{align*}
5 \cdot 2 &\equiv 10 \pmod{11} \\
5 \cdot 2 &\equiv -1 \pmod{11} \\
5 \cdot 10 &\equiv -5 \pmod{11} \\
5 \cdot 10 &\equiv -6 \pmod{11}
\end{align*}
\]

4. $7n \equiv 4 \pmod{19}$

From before: $11 \cdot 7 \equiv 1 \pmod{19}$, so $44 \cdot 7 \equiv 4 \pmod{19}$. Then $44 \mod 19 = 6$, so $6 \cdot 7 \equiv 4 \pmod{19}$.

5. $19n \equiv 1 \pmod{7}$

From before: $3 \cdot 19 - 8 \cdot 7 = 1$, so $19 \cdot 3 \equiv 1 \pmod{7}$.

6. $8n \equiv 8 \pmod{31}$

$31$ is prime, so $8n \equiv 8 \pmod{31} \iff n \equiv 1 \pmod{31}$.
7. $8n \equiv 18 \pmod{24}$

8 and 24 are both divisible by 8 but 18 is not. The system has no solutions.

8. $7n \equiv 18 \pmod{35}$

7 and 35 are both divisible by 7 but 18 is not. No solutions.

9. $7n \equiv 21 \pmod{35}$

All numbers are divisible by 7, so divide by 7 all around to get $n \equiv 3 \pmod{5}$. Mod 35, the solutions are $n = 3, 8, 13, 18, 23, 28, 33$.

10. $3n \equiv 9 \pmod{15}$

Divide by 3 to get $n \equiv 3 \pmod{5}$. Mod 15, the solutions are $n = 3, 8, 13$.

11. $15n \equiv 13 \pmod{25}$

15 and 25 are divisible by 5 but 13 is not. No solutions.

12. $15n \equiv 20 \pmod{25}$

Divide by 5 to get $3n \equiv 4 \pmod{5}$, which has the solution $n \equiv 3 \pmod{5}$. Mod 25, the solutions are $n = 3, 8, 13, 18, 23$.

**Chinese Remainder Theorem**

Decide whether the system has a solution. If it does, find it.

1. $x \equiv 3 \pmod{8}$, $x \equiv 1 \pmod{7}$

   Try $x = 8a + 7b$. mod 8, we get $3 \equiv x \equiv 7b$ (mod 8), and solving gives $b = 5$. mod 7, we get $1 \equiv x \equiv 8a$ (mod 7), so $a \equiv 1$ (mod 7). Therefore one solution is $x = 8 + 7 \cdot 5 = 43$.

2. $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{13}$

   Try $x = 5a + 13b$. mod 5, we get $2 \equiv x \equiv 13b \equiv 3b$ (mod 5), so $b = 4$ is a solution. mod 13, we get $3 \equiv x \equiv 5a$ (mod 13) with $a = 11$ as a solution. Therefore one solution is $11 \cdot 5 + 4 \cdot 13 = 107$, which is equivalent to 42 (mod 65).

3. $x \equiv 7 \pmod{6}$, $x \equiv 4 \pmod{8}$

   The first equation suggests that $x$ is odd but the second requires $x$ to be even. No solutions.

4. $x \equiv 1 \pmod{6}$, $x \equiv 5 \pmod{8}$

   Since $\gcd(6, 8) = 2$ but both equations give $x \equiv 1 \pmod{2}$, the equations are compatible. $x$ must be odd, so say $x = 2k + 1$. This leads to the equations $2k \equiv 0 \pmod{6}$ and $2k \equiv 4 \pmod{8}$, and dividing by 2 gives $k \equiv 0 \pmod{3}$ and $k \equiv 2 \pmod{4}$, with the solution $k = 6$. Thus $x = 2k + 1 = 2 \cdot 6 + 1 = 13$ is a solution (and the only solution mod 24).

5. $x \equiv 8 \pmod{15}$, $x \equiv 3 \pmod{10}$, $x \equiv 1 \pmod{6}$

   The first equation implies $x \equiv 2 \pmod{3}$ but the second requires that $x \equiv 1 \pmod{3}$.

6. $x \equiv 2 \pmod{3}$, $x \equiv 5 \pmod{7}$, $x \equiv 3 \pmod{11}$

   Try a solution of the form $x = 3 \cdot 7 \cdot a + 3 \cdot 11 \cdot b + 7 \cdot 11 \cdot c$. Taking the remainders mod 3, 7, and 11 in turn gives the three equations $2 \equiv 77c \equiv 2c$ (mod 3) (so $c = 1$), $5 \equiv 33 \cdot b \equiv 5 \cdot b$ (mod 7) (so $b = 1$), and $3 \equiv 21 \cdot a \equiv -a$ (mod 11) (so $a = -3$).

   One solution is therefore $x = -3 \cdot 21 + 1 \cdot 33 + 1 \cdot 77 = 47$. This solution is also unique mod $3 \cdot 7 \cdot 11 = 231$. 


Decide whether the system has a solution (and if it does, find all solutions) by solving the system for each prime factor separately.

1. \( n^2 \equiv 11 \pmod{35} \)
   Working over each prime factor separately gives \( n^2 \equiv 1 \pmod{5} \) and \( n^2 \equiv 4 \pmod{7} \), so \( n = \pm 1 \pmod{5} \) and \( n = \pm 2 \pmod{7} \).
   Finding all solutions using the Chinese Remainder Theorem would be a real pain, so we’ll go by brute force: look at all the numbers that are \( \pm 2 \pmod{7} \) and see which ones are also \( \pm 1 \pmod{5} \) (that is, end in a 1, 4, 6, or 9):
   The options \( \pmod{35} \) are \( n = 2, 5, 9, 12, 16, 19, 23, 26, 30, 33 \). Of these, the ones that work \( \pmod{5} \) are 9, 16, 19, and 26.

2. \( n^2 \equiv 12 \pmod{15} \)
   Get the equations \( n^2 \equiv 0 \pmod{3} \) and \( n^2 \equiv 2 \pmod{5} \)... the second equation has no solutions, so there are no solutions to \( n^2 \equiv 12 \pmod{15} \).

3. \( n^2 \equiv 15 \pmod{77} \)
   Get the equations \( n^2 \equiv 1 \pmod{7} \) and \( n^2 \equiv 4 \pmod{11} \), so \( n = \pm 1 \pmod{7} \) and \( n = \pm 2 \pmod{11} \). Look at the ones that work \( \pmod{11} \) and then filter out to see which work for 7:
   The options are \( n = 2, 9, 13, 20, 24, 31, 35, 42, 46, 53, 57, 64, 68, 75 \). Of these, 13, 20, 57, and 64 are \( \pm 1 \pmod{7} \). These are the four solutions.
   Note: \( 13 + 64 = 20 + 57 = 77 \), so these solutions again come in pairs. (That is, if \( n^2 \equiv 15 \pmod{77} \) then \( (-n)^2 \equiv 15 \pmod{77} \).)

4. \( n^2 \equiv 5 \pmod{33} \)
   This leads to the equation \( n^2 \equiv 2 \pmod{3} \), which has no solutions.

Show that if \( p \) and \( q \) are primes with \( p, q > 2 \) then \( n^2 \equiv 1 \pmod{pq} \) has four distinct solutions.

Use the Chinese Remainder Theorem on \( n \equiv \pm 1 \pmod{p} \), \( n \equiv \pm 1 \pmod{q} \).

---

**Fermat’s Little Theorem**

Evaluate:

1. \( 5^{100} \pmod{7} \)
   \( 5^6 \equiv 1 \pmod{7} \), so \( 5^{100} \equiv 5^4 \equiv (-2)^4 \equiv 16 \equiv 2 \pmod{7} \).

2. \( 3^{32} \pmod{5} \)
   \( 3^4 \equiv 1 \pmod{5} \) so \( 3^{32} \equiv 1 \pmod{5} \).

3. \( 17^{73} \pmod{19} \)
   \( 17^{18} \equiv 1 \pmod{19} \), so \( 17^{73} \equiv 17 \pmod{19} \).
4. $8^{32} \pmod{35}$

We cannot use Fermat’s Little Theorem directly, but we can solve mod 5 and mod 7 separately. $8^4 \equiv 1 \pmod{5}$, so $8^{32} \equiv 1 \pmod{5}$. Then $8 \equiv 1 \pmod{7}$ so $8^{32} \equiv 1 \pmod{7}$.

If $x \equiv 1 \pmod{5}$ and $x \equiv 1 \pmod{7}$ then $x \equiv 1 \pmod{35}$ (1 is a solution mod 35, and by CRT is the unique solution). Therefore $8^{32} \equiv 1 \pmod{35}$.

5. $8^{20} \pmod{15}$

$8 \equiv (-1) \pmod{3}$ so $8^{20} \equiv 1 \pmod{3}$. $8^4 \equiv 1 \pmod{5}$ so $8^{20} \equiv 1 \pmod{5}$. Putting the two together, $8^{20} \equiv 1 \pmod{15}$.

6. $15^{37} \pmod{21}$

$15$ is divisible by $3$ so $15^{37} \equiv 0 \pmod{3}$. $15$ is $1 \pmod{7}$ so $15^{37} \equiv 1 \pmod{7}$. Therefore $15^{37} \equiv 15 \pmod{21}$.

Show that $n^2 \equiv -1 \pmod{103}$ has no solutions.

FLT says that if $n \neq 0 \pmod{103}$ then $n^{102} \equiv 1 \pmod{103}$. But if $n^2 \equiv -1$ then $n^4 \equiv 1$, so $n^{100} \equiv 1 \pmod{103}$. So $n^{100} \equiv n^{102} \pmod{103}$ and so $n^2 \equiv 1 \pmod{103}$. Therefore there are no solutions to $n^2 \equiv -1 \pmod{103}$.

Use Fermat’s Little Theorem with base $n = 2$ to prove that $9$ is not prime.

$2^8 \equiv 4^4 \equiv 16^2 \equiv (-2)^2 \equiv 4 \neq 1 \pmod{9}$.

Use Wilson’s Theorem to show that $7$ is prime.

$6! = 120 = 119 + 1 = 17 \cdot 7 + 1 \equiv 1 \pmod{7}$, so $7$ is prime.