[redacted]

Solving congruences

Consider the function

$$f(x) \ = \ 7x + 4 \mod 12.$$

The implied domain of this function is the set of integers, and the codomain is the list of remainders $\{0, 1, 2, \ldots, 11\}$ which are possible when dividing an integer by 12. That is, the codomain is $\mathbb{Z}_{12}$. When we look to *solve* the (congruence) equation

$$7x + 4 \equiv 9 \pmod{12}, \tag{1}$$

we seek to describe those inputs x to f which produce the particular output 9.

From these facts

1. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.
2. If $a \equiv b \pmod{m}$ and $c \in \mathbb{Z}$, then $ac \equiv bc \pmod{m}$.

we know that we can perform some of the basic steps of algebra. With regards to the example equation (1), we solve by

- adding 8 to both sides, which gets rid of the $+4$ since $(8 + 4) \mod 12 = 0$

$$\left.\begin{array}{ll} \text{new LHS}: & 7x + 4 + 8 \equiv 7x + 12 \equiv 7x \pmod{12} \\ \text{new RHS}: & 9 + 8 \equiv 17 \equiv 5 \pmod{12} \end{array}\right\} \quad \Rightarrow \quad 7x \equiv 1 \pmod{12}.$$

- multiplying both sides by 7, since $(7 \cdot 7) \mod 12 = 1$.

$$\left.\begin{array}{ll} \text{new LHS}: & 7 \cdot 7x \equiv 49x \equiv x \pmod{12} \\ \text{new RHS}: & 7 \cdot 5 \equiv 11 \pmod{12} \end{array}\right\} \quad \Rightarrow \quad x \equiv 11 \pmod{12}.$$

These two steps have led to the solution: the integers x which satisfy Equation (1) are those which are equivalent to $11 \pmod{12}$.

The general linear congruence equation, with modulus $m \geqslant 2$, looks like

$$ax + b \equiv n \pmod{m}. \tag{2}$$

It can be solved in much the same way as above—adding $(-b)$, the **additive inverse** of b, to both sides, then multiplying by the **multiplicative inverse** of a—provided that [redacted] $\gcd(a, m) = 1$ (a sufficient condition for a to *have* a multiplicative inverse $\pmod{m}$).

Modular Arithmetic in check digits

ISBN-10 nos.

381X52314 ____

$x_1 = 3,\ x_2 = 8,\ x_3 = 1,\ x_4 = 10,\ \ldots,\ x_9 = 4,\ x_{10} = ?$

To find x_{10}, use that any valid ISBN-10 satisfies

$$\sum i x_i \bmod 11 = 0.$$

Can compute

$$1(3) + 2(8) + 3(1) + 4(10) + 5(5) + 6(2)$$
$$+ 7(3) + 8(1) + 9(4) + 10x_{10} \bmod 11$$

$$= -1 + 10x_{10} \bmod 11 = 0$$

So, I'm trying to solve $\quad 10x - 1 \equiv 0 \pmod{11}$

or $\quad 10x \equiv 1 \pmod{11}.$

Can reliably finish this, but also more generally equations like

$$ax + b \equiv c \pmod{m}$$

whenever I can find multi. inv. of $a \pmod{m}$.

Fact: $a \in \mathbb{Z}_m$ has a multiplicative inverse iff $\gcd(a,m) = 1$.

Ex.) (a) Use Euclidean algorithm to find $\gcd(34, 315)$.

$r_0 = 315, \quad r_1 = 34$

(1) $315 = 34 \cdot \underline{9} + \underline{9}, \qquad r_2 = 9$

(2) $34 = 9 \cdot \underline{3} + \underline{7} \qquad r_3 = 7$

(3) $9 = 7 \cdot \underline{1} + \underline{2} \qquad r_4 = 2$

(4) $7 = 2 \cdot \underline{3} + \underline{1} \qquad r_5 = 1 = \gcd(34, 315)$

(b) Use the extended EA to write $\gcd(34, 315)$ as a weighted sum

$t r_0 + s r_1 \qquad (s, t \in \mathbb{Z})$.

(4) rewritten becomes

$$1 = 7 - 2 \cdot 3 \qquad \text{or} \qquad 1 = r_3 - 3r_4 \quad (\star)$$

(3) $9 = 7 \cdot \underline{1} + \underline{2}$ can be rewritten to say

$$2 = 9 - 7 \qquad \text{or} \qquad r_4 = \underbrace{r_2 - r_3}$$

Can insert this for r_4 in $(\star)$

$$1 = r_3 - 3r_4 \quad \text{becomes} \quad 1 = r_3 - 3(r_2 - r_3)$$

Combining like terms:

$$1 = 4r_3 - 3r_2 \qquad (\star\star)$$

Next, (2) $34 = 9 \cdot \underline{3} + \underline{7}$ can be rewritten to say

$$7 = 34 - (3)(9) \quad \text{or} \quad r_3 = \underbrace{r_1 - 3r_2}_{\substack{\text{insert as } r_3 \\ \text{in } (\star\star)}}$$

$$1 = 4r_3 - 3r_2 \quad \text{becomes} \quad 1 = 4(r_1 - 3r_2) - 3r_2$$

or

$$1 = 4r_1 - 15r_2 \qquad (\star\star\star)$$

Finally, (1) $315 = 34 \cdot \underline{9} + \underline{9}$ can be rewritten as

$$9 = 315 - (9)(34) \quad \text{or,} \quad r_2 = \underbrace{r_0 - 9r_1}_{\substack{\text{insert as } r_2 \\ \text{in } (\star\star\star)}}$$

$$1 = 4r_1 - 15r_2 \quad \text{becomes} \quad 1 = 4r_1 - 15(r_0 - 9r_1)$$

$$1 = 139r_1 - 15r_0$$

Upshot $\quad 1 = (139)(34) - (15)(315)$

(c) What is mult. inv. of 34 in $\mathbb{Z}_{315}$?

Ans.: 139, since

$$(139)(34) = 315\,\underline{15} + \underline{1}$$

(d) Solve the congruence for x:

$$34x \equiv 8 \pmod{315}$$

Knowing 34 has mult. inv. 139, multiply both sides by it:

$$34x \equiv 8 \pmod{315}$$

$$(139)(34)x \equiv 1x \equiv (139)(8) \equiv 1112$$

$$x \equiv 167 \bmod (315)$$

You try: (a) Write $\gcd(39, 200)$ as weighted sum $t \cdot 200 + s \cdot 39$

$$1 = \gcd(39, 200) = 8(200) - 41(39)$$

(b) Does 39 have a mult. inv. mod 200? A: Yes.

(c) In terms of "representative" nos. mod 200

$$\mathbb{Z}_{200} = \{0, 1, 2, \ldots, 199\},$$

what <u>is</u> the mult. inv. of 39?

$-41 \equiv 159 \bmod (200)$, so 159 is 39's mult. inv.

For small integers a, m it is generally possible to figure out

- what the $\gcd(a, m)$ is, and
- when $\gcd(a, m) = 1$, which number $\bar{a} \in \mathbb{Z}_m$ is the multiplicative inverse—i.e., satisfies $a\bar{a} \equiv 1 \pmod{m}$.

When these cannot be determined so easily, we resort to the Euclidean and Extended Euclidean Algorithms.[1]

Example 3:

Show that the integers 311 and 6215 are relatively prime, and then find the multiplicative inverse of $311 \pmod{6215}$.

Answer: We perform steps of the Euclidean algorithm (left side) and, rewrite (right side) the equations to express the newest remainder r_j in terms of two prior ones r_{j-1} and r_{j-2} (helpful steps for the extended Euclidean algorithm):

$$\begin{array}{lcl} 6215 = (19)(311) + 306 & \Rightarrow & 306 = (1)(6215) - (19)(311) \\ 311 = (1)(306) + 5 & & 5 = (1)(311) - (1)(306) \\ 306 = (61)(5) + 1 & & 1 = (1)(306) - (61)(5) \\ 5 = (5)(1) + 0 & & \end{array}$$

The last nonzero remainder is $\gcd(6215, 311)$, and since it is 1, the two numbers are relatively prime.

To find the multiplicative inverse, we use the equations, starting at the bottom, on the right-hand side, continually substituting the next-higher equation:

$$\begin{aligned} 1 &= (1)(306) - (61)(5) \qquad \text{(bottom equation on the right)} \\ &= (1)(306) - (61)[(1)(311) - (1)(306)] \;=\; (62)(306) - (61)(311) \\ &= (62)[(1)(6215) - (19)(311)] - (61)(311) \;=\; (62)(6215) - (1239)(311) \\ &= (62)(6215) + (-1239)(311) \end{aligned}$$

If we consider the operations above as happening $\pmod{6215}$, we have

$$(62)(6215) + (-1239)(311) \equiv (4976)(311) \equiv 1 \pmod{6215}.$$

Thus, 4976 is the multiplicative inverse $\pmod{6215}$ of 311.

■

Example 4: Affine ciphers

[1] An app that implements both the Euclidean and Extended Euclidean Algorithms is linked to the class webpage. The direct url is `https://www.extendedeuclideanalgorithm.com/calculator.php`.

Affine ciphers are based on functions of the form

$$f(x) := ax + b \mod 26.$$

When $\gcd(a, 26) = 1$, such a function $f\colon \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ is *bijective* and is, thus, *invertible*.

One equates the 26 letters of the English alphabet with the numbers 0–25: $a \leftrightarrow 0$, $b \leftrightarrow 1, \ldots,$ $z \leftrightarrow 25$. This makes a natural map between simple strings of letters and finite sequences of integers, such as

$$\text{the word } \textit{pencil} \quad \leftrightarrow \quad 15, 4, 13, 2, 8, 11,$$

which, in its numerical equivalent, could hardly be said to be "encrypted." However, if we let $y = f(x)$, then an encrypted version of $x_1, x_2, x_3, x_4, x_5, x_6$ would be $y_1, y_2, y_3, y_4, y_5, y_6$, with

$$\begin{aligned}
x_1 = 15 &: \quad y_1 = f(15) = 15a + b \mod 26,\\
x_2 = 4 &: \quad y_2 = f(4) = 4a + b \mod 26,\\
x_3 = 13 &: \quad y_3 = f(13) = 13a + b \mod 26,\\
x_4 = 2 &: \quad y_4 = f(2) = 2a + b \mod 26,\\
x_5 = 8 &: \quad y_5 = f(8) = 8a + b \mod 26,\\
x_6 = 11 &: \quad y_6 = f(11) = 11a + b \mod 26.
\end{aligned}$$

In the case where $a = 19$ and $b = 4$, these encrypted values would be $3, 2, 17, 16, 0, 5$, though we would generally transmit this as its alphabetic equivalent *dcrqaf*.

The person on the receiving end needs the inverse function to f in order to perform decryption of the message. We can obtain it in the same manner described above—by solving the congruence equation $ax + b \equiv y \pmod{26}$. If $\bar{a}$ is the multiplicative inverse of $a \pmod{26}$, then

$$ax + b \equiv y \pmod{26} \qquad \Rightarrow \qquad x \equiv \bar{a}(y - b) \pmod{26}.$$

One needs $\gcd(a, 26) = 1$, of course, so that $\bar{a}$ exists, in which case $g(y) = \bar{a}(y - b) \mod 26$ is the inverse function to $f(x) = ax + b \mod 26$.

You can explore affine ciphers without the tedium of all the letter-to-number conversions at http://www.calvin.edu/~scofield/courses/m100/materials/scriptForms/affineTranslator.shtml a link which appears on the class webpage. While affine ciphers are a neat application of congruences, they are quite easily broken.

■

Systems of linear congruences

A **system of congruences** is nothing more than multiple individual congruences, with the requirement that any solution x must be an integer which simultaneously satisfies them all. First, an