Solutions to Daily Due Aug 31 (AI generated)

Math 4440/5440, Coding and Cryptography, Fall 2026

Generated by Claude for Katherine E. Stange
(methods follow the Fall 2024 lecture notes; all computations computer-verified)

Problem 2: quick review

The inverse of 7 **modulo** 11 **is** 8, since $7 \cdot 8 = 56 = 5 \cdot 11 + 1 \equiv 1 \pmod{11}$.

The inverse of 7 **modulo** 14 **does not exist.** This is the trick question: $\gcd(7, 14) = 7 \neq 1$, so 7 is not invertible modulo 14. (Directly: $7x$ is always 0 or 7 modulo 14, never 1.)

Problem 3: unit groups and $\varphi(n)$

$(\mathbb{Z}/n\mathbb{Z})^*$ is the set of residues coprime to n.

n	$(\mathbb{Z}/n\mathbb{Z})^*$	$\varphi(n)$
12	$\{1, 5, 7, 11\}$	4
15	$\{1, 2, 4, 7, 8, 11, 13, 14\}$	8
16	$\{1, 3, 5, 7, 9, 11, 13, 15\}$ (the odd residues)	8
26	$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ (odd, and not 13)	12
27	everything except $0, 3, 6, \ldots, 24$ (the non-multiples of 3)	18
30	$\{1, 7, 11, 13, 17, 19, 23, 29\}$	8

Notice that $\varphi(16) = 16 - 8$ (remove the evens), $\varphi(27) = 27 - 9$ (remove the multiples of 3), and $\varphi(26) = 26 - 13 - 2 + 1$ (remove the evens and the multiples of 13, but 0 was removed twice).

Problem 4: a badly chosen affine key

Take $\alpha = 2$ (not invertible modulo 26, since $\gcd(2, 26) = 2$) and any β, say $\beta = 0$. Then

$$\texttt{A} = 0 \mapsto 2 \cdot 0 = 0 = \texttt{A}, \qquad \texttt{N} = 13 \mapsto 2 \cdot 13 = 26 \equiv 0 = \texttt{A} \pmod{26},$$

so the two different plaintexts `A` and `N` both encrypt to `A`. (More generally, with $\alpha = 2$ any two letters 13 apart collide: `B` and `O`, `C` and `P`, ...)

The reason: encryption $x \mapsto \alpha x + \beta$ can be undone only if we can divide by α. When α is not invertible, the map $x \mapsto \alpha x$ is not injective, so decryption is ambiguous.

Problem 5: powers of a modulo n

(a) Some power repeats. The list $a, a^2, a^3, \ldots$ is infinite, but each entry is one of the n residues $0, 1, \ldots, n-1$. By the pigeonhole principle, two entries (in fact, among the first $n+1$ entries) must be equal: $a^i \equiv a^j \pmod{n}$ for some $i < j$.

(b) If a is invertible, some power is 1. Take $i < j$ with $a^i \equiv a^j$ from part (a). Since a is invertible, so is a^i (its inverse is $(a^{-1})^i$). Multiplying both sides by $(a^{-1})^i$ cancels a^i:

$$1 \equiv a^{j-i} \pmod{n}, \qquad j - i \geq 1.$$

So $a^k \equiv 1$ with $k = j - i$. (This is the "cancellation" from the Aug 26 daily post: you may cancel an invertible factor.)

(c) A residue no power of which is 1. Take $a = 2$ modulo $n = 4$: the powers are $2, 0, 0, 0, \ldots$, never 1. (Or $a = 0$, or $a = 6$ modulo 10: $6, 6, 6, \ldots$)

In fact *any* non-invertible a works: if $a^k \equiv 1$ for some $k \geq 1$, then $a \cdot a^{k-1} \equiv 1$ exhibits an inverse of a. So "some power of a is 1" happens *exactly* for the invertible residues.

Problem 6: Hill cipher

Encode $\texttt{A} = 0, \ldots, \texttt{Z} = 25$ and, as in the course tools, encrypt a block by multiplying a 2×2 key matrix K by the block written as a column vector.

(a) Recovering the key from $\texttt{SOLVED} \mapsto \texttt{GEZXDS}$. The plaintext blocks are

$$\texttt{SO} = \begin{pmatrix} 18 \\ 14 \end{pmatrix}, \qquad \texttt{LV} = \begin{pmatrix} 11 \\ 21 \end{pmatrix}, \qquad \texttt{ED} = \begin{pmatrix} 4 \\ 3 \end{pmatrix},$$

encrypting respectively to

$$\texttt{GE} = \begin{pmatrix} 6 \\ 4 \end{pmatrix}, \qquad \texttt{ZX} = \begin{pmatrix} 25 \\ 23 \end{pmatrix}, \qquad \texttt{DS} = \begin{pmatrix} 3 \\ 18 \end{pmatrix}.$$

Two blocks give the matrix equation $KP = C$, where P has the two plaintext blocks as columns and C the corresponding ciphertext blocks; then $K = CP^{-1}$, provided P is invertible modulo 26.

The first two blocks give $P = \begin{pmatrix} 18 & 11 \\ 14 & 21 \end{pmatrix}$ with $\det P = 378 - 154 = 224 \equiv 16 \pmod{26}$, and $\gcd(16, 26) = 2$ — not invertible, so try again. The last two blocks give

$$P = \begin{pmatrix} 11 & 4 \\ 21 & 3 \end{pmatrix}, \qquad \det P = 33 - 84 = -51 \equiv 1 \pmod{26},$$

which is invertible, and since the determinant is 1 the inverse is just the adjugate:

$$P^{-1} \equiv \begin{pmatrix} 3 & -4 \\ -21 & 11 \end{pmatrix} \equiv \begin{pmatrix} 3 & 22 \\ 5 & 11 \end{pmatrix} \pmod{26}.$$

Therefore

$$K = CP^{-1} = \begin{pmatrix} 25 & 3 \\ 23 & 18 \end{pmatrix} \begin{pmatrix} 3 & 22 \\ 5 & 11 \end{pmatrix} = \begin{pmatrix} 90 & 583 \\ 159 & 704 \end{pmatrix} \equiv \begin{pmatrix} 12 & 11 \\ 3 & 2 \end{pmatrix} \pmod{26}.$$

Check on the block we didn't use: $K\binom{18}{14} = \binom{216+154}{54+28} = \binom{370}{82} \equiv \binom{6}{4} = \texttt{GE}$. ✓ (And $\det K = 24 - 33 = -9 \equiv 17$, coprime to 26, so this is a legal key.)

If you instead write blocks as row vectors and multiply on the right, your key is the transpose $\begin{pmatrix} 12 & 3 \\ 11 & 2 \end{pmatrix}$.

(b) The matrix $M = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ modulo 26. Its determinant is $4 - 6 = -2 \equiv 24$, and $\gcd(24, 26) = 2$, so M is *not* invertible modulo 26. Concretely, we can find a nonzero block that encrypts to $\binom{0}{0}$:

$$M\begin{pmatrix} 0 \\ 13 \end{pmatrix} = \begin{pmatrix} 26 \\ 52 \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{26}.$$

So $\texttt{AN} = \binom{0}{13}$ and $\texttt{AA} = \binom{0}{0}$ both encrypt to $\texttt{AA}$. (Adding $\binom{0}{13}$ to *any* block leaves its ciphertext unchanged, so every ciphertext has two plaintexts: e.g. $\texttt{HI}$ and $\texttt{HV}$ collide.)

What's wrong: the determinant shares a factor with 26 (it is even), so encryption is not injective and there is no decryption matrix. A Hill key must have $\gcd(\det K, 26) = 1$.

Problem 7: double-and-add for 2^{148}

Write the exponent in binary: $148 = 128 + 16 + 4 = 10010100_2$. Reading the bits from left to right, start with exponent 0 and, for each bit, *double* the exponent (square the running power) and then, if the bit is 1, *add* 1 (multiply by the base):

bit	exponent so far	running power
1	$0 \to 0 \to 1$	2^1
0	$1 \to 2$	$(2^1)^2 = 2^2$
0	$2 \to 4$	$(2^2)^2 = 2^4$
1	$4 \to 8 \to 9$	$(2^4)^2 \cdot 2 = 2^9$
0	$9 \to 18$	$(2^9)^2 = 2^{18}$
1	$18 \to 36 \to 37$	$(2^{18})^2 \cdot 2 = 2^{37}$
0	$37 \to 74$	$(2^{37})^2 = 2^{74}$
0	$74 \to 148$	$(2^{74})^2 = 2^{148}$

That is 7 squarings and 2 extra multiplications — 9 multiplications instead of 147. (Equivalently, successive squaring computes 2^4, 2^{16}, 2^{128} and multiplies them.) For the record,

$$2^{148} = 356811923176489970264571492362373784095686656.$$

The same recipe works modulo any n, reducing after each step, and it is the algorithm we will use constantly from now on.