Solutions to Daily Due Aug 28

Math 4440/5440, Coding and Cryptography, Fall 2026

Katherine E. Stange
(problem 5 from her 2024 lecture notes; the rest AI generated;
all computations computer-verified)

Problem 3: eavesdropping on your little sister

Encode $\texttt{A} = 0, \ldots, \texttt{Z} = 25$. Affine encryption is $x \mapsto \alpha x + \beta \pmod{26}$. We know the ciphertext `CRWWZ` and that the plaintext begins `HA`; this is a *known-plaintext attack*, and two letters are enough to pin down the two unknowns α, β.

Find the key. The pairs $\texttt{H} \mapsto \texttt{C}$ and $\texttt{A} \mapsto \texttt{R}$ say

$$7\alpha + \beta \equiv 2, \qquad 0 \cdot \alpha + \beta \equiv 17 \pmod{26}.$$

The second equation hands us $\beta = 17$. Substituting into the first,

$$7\alpha \equiv 2 - 17 \equiv -15 \equiv 11 \pmod{26}.$$

Since $7 \cdot 15 = 105 = 4 \cdot 26 + 1$, we have $7^{-1} \equiv 15$, so

$$\alpha \equiv 15 \cdot 11 = 165 \equiv 165 - 6 \cdot 26 = 9 \pmod{26}.$$

The key is $(\alpha, \beta) = (9, 17)$ — a legal key, since $\gcd(9, 26) = 1$.

Decrypt. Decryption is $y \mapsto \alpha^{-1}(y - \beta) \pmod{26}$, and $9^{-1} \equiv 3$ (because $9 \cdot 3 = 27 \equiv 1$). Applying $y \mapsto 3(y - 17)$ to $\texttt{CRWWZ} = 2, 17, 22, 22, 25$:

$$3(2 - 17) \equiv -45 \equiv 7, \quad 3(0) = 0, \quad 3(5) = 15, \quad 3(5) = 15, \quad 3(8) = 24,$$

which is $7, 0, 15, 15, 24 = \texttt{HAPPY}$.

(Check: encrypting `HAPPY` with the key $(9, 17)$ gives back `CRWWZ`.)

Problem 4: inverses

- $2^{-1} \equiv 9 \pmod{17}$, because $2 \cdot 9 = 18 \equiv 1 \pmod{17}$.
- $8^{-1} \equiv 7 \pmod{11}$, because $8 \cdot 7 = 56 = 55 + 1 \equiv 1 \pmod{11}$.
- 3 has **no inverse** modulo 15, because $\gcd(3, 15) = 3 \neq 1$. To see the trouble directly: any multiple of 3 is still a multiple of 3 after reducing mod 15 (since 15 is itself a multiple of 3), so $3x$ can only ever be $0, 3, 6, 9$, or 12 — never 1. Equivalently, $3x \equiv 1 \pmod{15}$ would mean $3x + 15k = 1$ for some integer k, but the left side is divisible by 3 and 1 is not.

For the small moduli here, trial multiplication finds the inverses quickly; later in the course we'll meet an efficient algorithm (the extended Euclidean algorithm) for large moduli.

Problem 5: computing $3^{519} \pmod{11}$ by hand

The trick is to find a power of 3 that is $\equiv 1$, and it comes fast:

$$3^2 = 9, \qquad 3^4 = (3^2)^2 = 81 \equiv 4, \qquad 3^5 = 3^4 \cdot 3 \equiv 4 \cdot 3 = 12 \equiv 1 \pmod{11}.$$

That's the whole computation: **three multiplications** (square, square, times 3). Now divide the exponent: $519 = 5 \cdot 103 + 4$, so

$$3^{519} = \left(3^5\right)^{103} \cdot 3^4 \equiv 1^{103} \cdot 3^4 \equiv \mathbf{4} \pmod{11}.$$

Remark. Plain successive squaring (coming soon in class) writes $519 = 512 + 4 + 2 + 1$ and spends 9 squarings plus 3 extra multiplications — 12 in all. Spotting the cycle $3^5 \equiv 1$ beats it handily: the powers of 3 mod 11 just cycle through $3, 9, 5, 4, 1$ forever, and 3^{519} lands where 519 sits in the cycle, at $519 \equiv 4 \pmod{5}$.

Remark. Since $3^4 \cdot 3 \equiv 1$, the computation also shows $3^4 \equiv 3^{-1} \pmod{11}$: the answer 4 is the inverse of 3.