Solutions to Daily Due Sep 2 (AI generated)

Math 4440/5440, Coding and Cryptography, Fall 2026

Generated by Claude for Katherine E. Stange
(methods follow the Fall 2024 lecture notes of Sept 6 and 9; all computations computer-verified)

Problem 1: the formula for $\varphi(n)$

$\varphi(15) = 15\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 15\cdot\frac{2}{3}\cdot\frac{4}{5} = 8, \qquad \varphi(30) = 30\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 30\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5} = 8.$

Both agree with the counts from the last daily post: $(\mathbb{Z}/15\mathbb{Z})^* = \{1,2,4,7,8,11,13,14\}$ and $(\mathbb{Z}/30\mathbb{Z})^* = \{1,7,11,13,17,19,23,29\}$, eight elements each.

Problem 3: $3^{133} \pmod{1009}$ by successive squaring

First, $133 = 128 + 4 + 1 = 10000101_2$. Squaring repeatedly, reducing modulo 1009 at each step:

$$\begin{aligned}
3^1 &\equiv 3 \\
3^2 &\equiv 9 \\
3^4 &\equiv 81 \\
3^8 &\equiv 6561 \equiv 507 && (6561 = 6\cdot 1009 + 507) \\
3^{16} &\equiv 507^2 = 257049 \equiv 763 && (257049 = 254\cdot 1009 + 763) \\
3^{32} &\equiv 763^2 = 582169 \equiv 985 && (582169 = 576\cdot 1009 + 985) \\
3^{64} &\equiv 985^2 = 970225 \equiv 576 && (970225 = 961\cdot 1009 + 576) \\
3^{128} &\equiv 576^2 = 331776 \equiv 824 && (331776 = 328\cdot 1009 + 824)
\end{aligned}$$

Then

$$3^{133} = 3^{128}\cdot 3^4\cdot 3^1 \equiv 824\cdot 81\cdot 3 \pmod{1009}.$$

Now $824\cdot 81 = 66744 = 66\cdot 1009 + 150 \equiv 150$, and $150\cdot 3 = 450$. So

$$3^{133} \equiv \mathbf{450} \pmod{1009}.$$

(Double-and-add gives the same answer with the same eight squarings.)

Problem 4: fun modular arithmetic, part one

1. 7 is prime and $12 = 2^2\cdot 3$; they share no prime factor, so $\gcd(7,12) = 1$.
2. $\varphi(12) = 12\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 4$; indeed $(\mathbb{Z}/12\mathbb{Z})^* = \{1,5,7,11\}$.
3. Euler's theorem says that if $\gcd(a,n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod{n}$. Here it says $7^4 \equiv 1 \pmod{12}$, so the powers of 7 repeat with period dividing 4 — exponents of 7 "live modulo 4". We checked coprimality because the theorem *requires* it (see Problem 7), and we computed $\varphi(12)$ because that is the exponent the theorem hands us.

4. Since $7^4 \equiv 1$, reduce the exponent modulo 4: $115 = 4 \cdot 28 + 3$, so

$$7^{115} = (7^4)^{28} \cdot 7^3 \equiv 7^3 = 343 = 28 \cdot 12 + 7 \equiv \mathbf{7} \pmod{12}.$$

(Even faster: $7^2 = 49 \equiv 1 \pmod{12}$, so $7^{115} = 7^{114} \cdot 7 \equiv 7$.)

Problem 5: fun modular arithmetic, part two

1. 59 is prime and $26 = 2 \cdot 13$, so $\gcd(59, 26) = 1$.
2. $\varphi(26) = 26\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{13}\right) = 26 \cdot \frac{1}{2} \cdot \frac{12}{13} = 12$. (Sage: `euler_phi(26)` returns `12`.)
3. By Euler's theorem, $59^{12} \equiv 1 \pmod{26}$, so the exponent 7^{115} only matters modulo 12. And $7^{115} \equiv 7 \pmod{12}$ is exactly Problem 4(d)! Hence

$$59^{(7^{115})} \equiv 59^7 \pmod{26}.$$

Also $59 = 2 \cdot 26 + 7 \equiv 7 \pmod{26}$, so we want $7^7 \pmod{26}$:

$$7^2 = 49 \equiv 23 \equiv -3, \qquad 7^4 \equiv (-3)^2 = 9 \pmod{26},$$

so

$$7^7 = 7^4 \cdot 7^2 \cdot 7 \equiv 9 \cdot (-3) \cdot 7 = -189 \equiv -189 + 8 \cdot 26 = \mathbf{19} \pmod{26}.$$

Problem 6: $3^{(11^{200006})} \pmod{50}$

Attack the outer power first. Since $\gcd(3, 50) = 1$ and $\varphi(50) = 50\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 20$, Euler's theorem gives $3^{20} \equiv 1 \pmod{50}$: the exponent 11^{200006} only matters modulo 20.

So now compute $11^{200006} \pmod{20}$. Since $\gcd(11, 20) = 1$ and $\varphi(20) = 20 \cdot \frac{1}{2} \cdot \frac{4}{5} = 8$, we have $11^8 \equiv 1 \pmod{20}$, and $200006 = 8 \cdot 25000 + 6$, so

$$11^{200006} \equiv 11^6 \pmod{20}.$$

And $11^2 = 121 = 6 \cdot 20 + 1 \equiv 1 \pmod{20}$, so $11^6 = (11^2)^3 \equiv 1 \pmod{20}$.

Returning to the original problem: the exponent is $\equiv 1 \pmod{20}$, so

$$3^{(11^{200006})} \equiv 3^1 = \mathbf{3} \pmod{50}.$$

Problem 7: does $3^8 \equiv 6 \pmod{15}$ contradict Euler?

Both facts are correct: $\varphi(15) = 8$, and $3^8 = 6561 = 437 \cdot 15 + 6 \equiv 6 \pmod{15}$.

There is no contradiction because Euler's theorem only applies when $\gcd(a, n) = 1$, and here $\gcd(3, 15) = 3$. The residue 3 is not in $(\mathbb{Z}/15\mathbb{Z})^*$, so no power of 3 can ever be 1 modulo 15 (see Problem 5(c) of the last daily post): its powers are $3, 9, 12, 6, 3, 9, 12, 6, \ldots$, cycling without ever visiting 1. This is why every use of Euler's theorem above began with a coprimality check.