Solutions to Daily Due Sep 14 (AI generated)

Math 4440/5440, Coding and Cryptography, Fall 2026

Generated by Claude for Katherine E. Stange
(all computations computer-verified)

Problems 1, 2, 3 and 7 are reminders and reading. Throughout, $p = 131$, $g = 2$, and $L(a)$ denotes the discrete logarithm of a base 2, which is only defined modulo $p - 1 = 130 = 2 \cdot 5 \cdot 13$.

Problem 4: $2^x \equiv 17 \pmod{131}$ by the Index Calculus

Because the algorithm is randomized, everyone's relations will differ; here is one complete run. Take the factor base $\{2, 3, 5, 7\}$. Of course $L(2) = 1$.

Phase 1: relations. Powers of 2 modulo 131 that factor over the base include

$$2^8 \equiv 125 = 5^3, \qquad 2^{12} \equiv 35 = 5 \cdot 7, \qquad 2^{38} \equiv 21 = 3 \cdot 7 \pmod{131}.$$

Taking logs, these say

$$8 \equiv 3L(5), \qquad 12 \equiv L(5) + L(7), \qquad 38 \equiv L(3) + L(7) \pmod{130}.$$

Phase 1: solve the linear system. Since $\gcd(3, 130) = 1$ we may divide by 3: the inverse of 3 modulo 130 is 87 (check: $3 \cdot 87 = 261 = 2 \cdot 130 + 1$). So

$$L(5) \equiv 8 \cdot 87 = 696 \equiv 46 \pmod{130}.$$

Subtracting the first relation from the second, $L(7) \equiv 12 - 46 = -34 \equiv 96$. Subtracting again, $L(3) \equiv 38 - 96 = -58 \equiv 72$.

Check: $2^{46} \equiv 5$, $2^{96} \equiv 7$ and $2^{72} \equiv 3 \pmod{131}$.

Phase 2: bring in $h = 17$. Multiply 17 by powers of 2 until the result factors over the base:

$$17 \cdot 2^3 = 136 \equiv 5 \pmod{131}.$$

So $L(17) + 3 \equiv L(5) = 46$, giving

$$\boxed{x = L(17) = 43}, \qquad \text{and indeed } 2^{43} \equiv 17 \pmod{131}.$$

(Other phase-2 hits work equally well, e.g. $17 \cdot 2^{19} \equiv 49 = 7^2$ gives $L(17) \equiv 2 \cdot 96 - 19 = 173 \equiv 43$.)

Problem 5: an awkward linear system

(1) $2^7 = 128 \equiv -3 \pmod{131}$, *not* 3. So $L(3) = 7$ is wrong.

(2) We tried to divide $14 \equiv 2L(3) \pmod{130}$ by 2, but 2 has no inverse modulo 130 because $\gcd(2, 130) = 2$. The congruence $2y \equiv 14 \pmod{130}$ says $130 \mid 2y - 14$, i.e. $65 \mid y - 7$, so it has **two** solutions modulo 130:

$$y \equiv 7 \quad \text{or} \quad y \equiv 7 + 65 = 72 \pmod{130}.$$

Since $2^7 \equiv -3$, the true value is $L(3) = 72$ (and indeed $2^{72} \equiv 3$). The two candidates differ by $65 = (p-1)/2$, and $2^{65} \equiv -1$, which is exactly why the wrong one produced -3.

(3) The parity test from the last daily post: $3^{65} \equiv 1 \pmod{131}$. If $L(3) = y$ then $3^{65} = 2^{65y} = (2^{65})^y = (-1)^y$, so $3^{65} \equiv 1$ means y is **even**. Of the two candidates 7 and 72, only 72 is even, so $L(3) = 72$ with no further checking.

(4) Using $2^8 \equiv 5^3$, $2^{12} \equiv 5 \cdot 7$, $2^{38} \equiv 3 \cdot 7$: exactly as in Problem 4, $L(5) = 8 \cdot 3^{-1} = 8 \cdot 87 \equiv 46$, $L(7) = 12 - 46 \equiv 96$, and $L(3) = 38 - 96 \equiv 72 \pmod{130}$. The only division was by 3, a unit modulo 130. This agrees with part (3).

(5) You may divide by a modulo $p-1$ exactly when $\gcd(a, p-1) = 1$, i.e. when a is a unit modulo $p-1$. Here, with $130 = 2 \cdot 5 \cdot 13$, that means a is not divisible by 2, 5 or 13. Since $p-1$ is always even, you can *never* safely divide by 2 (or any even number); if you are forced to, you get two candidates and must decide between them, e.g. with the parity test.

Problem 6: runtime comparison

(1) With $p \approx 10^d$:

digits	$\sqrt{p}$ (BSGS)	$e^{\sqrt{\ln p \, \ln\ln p}}$ (Index Calculus)
20	1.0×10^{10}	5.9×10^{5}
40	1.0×10^{20}	7.3×10^{8}
100	1.0×10^{50}	2.3×10^{15}

For example, for $d = 40$: $\ln p = 40 \ln 10 = 92.10$, $\ln\ln p = 4.523$, $\sqrt{92.10 \times 4.523} = 20.41$, and $e^{20.41} \approx 7.3 \times 10^8$.

(2) Against Baby-Step Giant-Step we need $\sqrt{p} > 10^{20}$, i.e. $p > 10^{40}$: **about 40 digits** (more, to be comfortable). Against the Index Calculus we need $e^{\sqrt{\ln p \, \ln\ln p}} > 10^{20}$; solving numerically, the formula crosses 10^{20} between 156 and 157 digits (9.2×10^{19} at 156 digits, 1.1×10^{20} at 157). So p needs **about 157 digits**, roughly four times as many.

(3) Write both as powers of e. Any fixed power $p^\varepsilon = e^{\varepsilon \ln p}$ has exponent proportional to $\ln p$, but the Index Calculus exponent is $\sqrt{\ln p \cdot \ln\ln p}$, and

$$\frac{\sqrt{\ln p \, \ln\ln p}}{\varepsilon \ln p} = \frac{1}{\varepsilon}\sqrt{\frac{\ln\ln p}{\ln p}} \longrightarrow 0 \quad \text{as } p \to \infty.$$

So the Index Calculus is eventually faster than p^ε for *every* $\varepsilon > 0$ (slower than exponential in the number of digits), yet it is still faster-growing than any polynomial in $\ln p$ (because $\sqrt{\ln p \ln\ln p}$ beats $c \ln\ln p$). That in-between growth is what *subexponential* means.