Solutions to Daily Due Sep 30 (AI generated)

Math 4440/5440, Coding and Cryptography, Fall 2026

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

Problem 1 was to watch the videos; the solutions below cover problems 2–10. Conventions as in lecture: each step of the Euclidean algorithm is a row $a = qb + r$; for the extended algorithm, every number d in the rows gets a "recipe card" (x, y) meaning $ax + by = d$ (with a, b the original inputs). The first row's cards are $(1, 0)$ for a and $(0, 1)$ for b, and since each remainder is $r =$ (left) $-\, q \cdot$ (middle), its card is the left card minus q times the middle card.

Problem 2: $\gcd(135, 170)$

$$\begin{aligned} 170 &= 1 \cdot 135 + 35 \\ 135 &= 3 \cdot 35 + 30 \\ 35 &= 1 \cdot 30 + 5 \\ 30 &= 6 \cdot 5 + 0 \end{aligned}$$

The last nonzero remainder is $\gcd(135, 170) = 5$.

Problem 3: $7x + 15y = 1$ by inspection

$15 = 2 \cdot 7 + 1$ says $7 \cdot (-2) + 15 \cdot 1 = 1$, so $(x, y) = (-2, 1)$ works.

Read it modulo 15: $7 \cdot (-2) \equiv 1$, so the inverse of 7 modulo 15 is $-2 \equiv 13$. (Check: $7 \cdot 13 = 91 = 6 \cdot 15 + 1$.)

Read it modulo 7: $15 \cdot 1 \equiv 1$, so the inverse of 15 modulo 7 is 1. (Of course: $15 \equiv 1 \pmod 7$.)

Problem 4: $\gcd(183, 105)$

$$\begin{aligned} 183 &= 1 \cdot 105 + 78 \\ 105 &= 1 \cdot 78 + 27 \\ 78 &= 2 \cdot 27 + 24 \\ 27 &= 1 \cdot 24 + 3 \\ 24 &= 8 \cdot 3 + 0 \end{aligned}$$

So $\gcd(183, 105) = 3$. Sage: `gcd(183,105)` returns `3`.

Problem 5: $183x + 105y = 3$ with recipe cards

Here $a = 183$ and $b = 105$. The cards, worked from the top down:

row	cards			check
$183 = 1 \cdot 105 + 78$	$(1, 0)$	$(0, 1)$	$(1, -1)$	$183 \cdot 1 + 105 \cdot (-1) = 78$
$105 = 1 \cdot 78 + 27$	$(0, 1)$	$(1, -1)$	$(-1, 2)$	$183 \cdot (-1) + 105 \cdot 2 = 27$
$78 = 2 \cdot 27 + 24$	$(1, -1)$	$(-1, 2)$	$(3, -5)$	$183 \cdot 3 + 105 \cdot (-5) = 24$
$27 = 1 \cdot 24 + 3$	$(-1, 2)$	$(3, -5)$	$(-4, 7)$	$183 \cdot (-4) + 105 \cdot 7 = 3$
$24 = 8 \cdot 3 + 0$	$(3, -5)$	$(-4, 7)$	$(35, -61)$	$183 \cdot 35 + 105 \cdot (-61) = 0$

For example, the card for 78 is $(1, 0) - 1 \cdot (0, 1) = (1, -1)$, and the card for 24 is $(1, -1) - 2 \cdot (-1, 2) = (3, -5)$. The card above the gcd is the answer:

$$183 \cdot (-4) + 105 \cdot 7 = -732 + 735 = 3, \qquad (x, y) = (-4, 7).$$

The last card is the free check: $183 \cdot 35 = 105 \cdot 61 = 6405$. Sage's `xgcd(183,105)` returns `(3, -4, 7)`.

Problem 6: the equation $3x + 5y = 0$, and then $= 1$

1. One solution: $(x, y) = (5, -3)$, since $15 - 15 = 0$. (Or the lazy one, $(0, 0)$.)
2. Another: $(-5, 3)$, or $(10, -6)$.
3. Infinitely many: $(x, y) = (5k, -3k)$ for any integer k, since $3 \cdot 5k + 5 \cdot (-3k) = 0$. (These are in fact all of them: $3x = -5y$ forces $5 \mid x$ since $\gcd(3, 5) = 1$.)
4. $3x + 5y = 1$: $(x, y) = (2, -1)$, since $6 - 5 = 1$. (From the algorithm: $5 = 1 \cdot 3 + 2$, $3 = 1 \cdot 2 + 1$, cards give $1 = 3 \cdot 2 - 5 \cdot 1$.)
5. Add any solution of the homogeneous equation to the particular one:

   $$(x, y) = (2 + 5k,\ -1 - 3k), \qquad k \in \mathbb{Z},$$

   e.g. $(2, -1)$, $(7, -4)$, $(12, -7)$, $(-3, 2)$, $(-8, 5)$. Check: $3(2 + 5k) + 5(-1 - 3k) = 6 + 15k - 5 - 15k = 1$.

Problem 7: the runtime of the Euclidean algorithm

One step sends (a, b) to $(a', b') = (b, a - qb) = (b, r)$ with $0 \le r < b$.

1. If $b < a/2$, then $b' = r < b < a/2$.
2. If $b \ge a/2$, then $q \ge 1$ and $b' = r = a - qb \le a - b \le a - a/2 = a/2$.
3. After one step the new first entry is $a' = b$, and after two steps the first entry is $a'' = b'$. By (1) and (2), $b' \le a/2$ in either case, so $a'' \le a/2$: every two steps, the first entry at least halves.

4. Starting from a, after $2t$ steps the first entry is at most $a/2^t$, and the algorithm must stop once that drops below 1. So the number of steps is at most about $2\log_2 a$: the runtime is $O(\log a)$ steps, i.e. linear in the number of *digits* (bits) of the input. Each step is a division of numbers with at most $\log a$ bits, so the total bit cost is polynomial in the input size. (The Euclidean algorithm is fast.)

Problem 8: Fibonacci inputs are the worst case

$$89 = 1\cdot 55 + 34, \quad 55 = 1\cdot 34 + 21, \quad 34 = 1\cdot 21 + 13,$$
$$21 = 1\cdot 13 + 8, \quad 13 = 1\cdot 8 + 5, \quad 8 = 1\cdot 5 + 3,$$
$$5 = 1\cdot 3 + 2, \quad 3 = 1\cdot 2 + 1, \quad 2 = 2\cdot 1 + 0.$$

That is 9 steps (the gcd is 1). Nearby pairs are much faster:

(a, b)	steps	gcd
$(89, 55)$	9	1
$(89, 56)$	6	1
$(90, 55)$	5	5
$(100, 63)$	7	1
$(97, 61)$	7	1
$(96, 64)$	2	32

Consecutive Fibonacci numbers are slow because every quotient is $q = 1$ (since $F_{n+1} = 1\cdot F_n + F_{n-1}$), the smallest possible, so each step removes as little as possible, and the remainders walk back down the Fibonacci sequence one term at a time. Any quotient ≥ 2 shrinks things faster. Compare with the bound from problem 7: $2\log_2 89 \approx 13$, and the actual 9 steps are below that but of the same order (Fibonacci numbers grow like ϕ^n with $\phi \approx 1.618$, so the true worst case is about $\log_\phi a \approx 1.44\log_2 a$ steps, which is ≈ 9.3 for $a = 89$). So the bound in problem 7 is the right shape, and the Fibonacci pairs show it can't be improved by more than a constant factor.

Problem 9: which c are $12x+42y$, and all solutions of $1071x+462y = 21$

Any $12x + 42y$ is a multiple of $\gcd(12, 42) = 6$, and conversely $6 = 12\cdot(-3) + 42\cdot 1$, so every multiple $6k = 12(-3k) + 42k$ is reachable. The answer: exactly the multiples of 6.

For $1071x + 462y = 21$:

$$1071 = 2\cdot 462 + 147$$
$$462 = 3\cdot 147 + 21$$
$$147 = 7\cdot 21 + 0$$

so $\gcd(1071, 462) = 21$ and the equation is solvable. Cards: 147 gets $(1, 0) - 2(0, 1) = (1, -2)$; 21 gets $(0, 1) - 3(1, -2) = (-3, 7)$; the 0 gets $(1, -2) - 7(-3, 7) = (22, -51)$. So one solution is

$$1071\cdot(-3) + 462\cdot 7 = -3213 + 3234 = 21, \qquad (x, y) = (-3, 7).$$

The last card gives the homogeneous solutions $(22k, -51k)$ (note $22 = 1071/21$ and $51 = 462/21$), so all integer solutions are

$$(x, y) = (-3 + 22k,\ 7 - 51k), \qquad k \in \mathbb{Z},$$

e.g. $(-25, 58)$, $(-3, 7)$, $(19, -44)$.

Problem 10: $\gcd(2^a - 1, 2^b - 1)$

Sage gives $\gcd(2^{12} - 1, 2^{18} - 1) = \gcd(4095, 262143) = 63 = 2^6 - 1$, and more data:

(a, b)	$\gcd(2^a - 1, 2^b - 1)$	$\gcd(a, b)$
$(12, 18)$	$63 = 2^6 - 1$	6
$(12, 30)$	$63 = 2^6 - 1$	6
$(20, 8)$	$15 = 2^4 - 1$	4
$(9, 6)$	$7 = 2^3 - 1$	3
$(7, 5)$	$1 = 2^1 - 1$	1

The guess: $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$.

Why. For $a > b$, the hint says $2^a - 1 = 2^{a-b}(2^b - 1) + (2^{a-b} - 1)$, so

$$\gcd(2^a - 1, 2^b - 1) = \gcd(2^b - 1, 2^{a-b} - 1)$$

(the usual fact that $\gcd(u, v) = \gcd(v, u - kv)$). The exponents (a, b) became $(b, a - b)$, which is one subtraction step of the Euclidean algorithm run on the exponents. Repeating, the exponents follow the Euclidean algorithm (subtraction version) all the way down to $(\gcd(a, b), 0)$, and $2^0 - 1 = 0$, so the gcd of the big numbers is $2^{\gcd(a,b)} - 1$. For the example: $(12, 18) \to (18, 12) \to (12, 6) \to (6, 6) \to (6, 0)$, giving $2^6 - 1 = 63$. Concretely, $262143 = 64 \cdot 4095 + 63$ and $4095 = 65 \cdot 63 + 0$.