Solutions to Daily Due Oct 5 (AI generated)

Math 4440/5440, Coding and Cryptography, Fall 2026

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

Problem 1: square roots modulo $p \equiv 3 \pmod 4$

Why $a^{(p-1)/2} \equiv 1$. Since a is a square modulo p, write $a \equiv b^2$ with $p \nmid b$. Then by Fermat's little theorem

$$a^{(p-1)/2} \equiv (b^2)^{(p-1)/2} = b^{p-1} \equiv 1 \pmod p.$$

(Note $(p-1)/2$ is an integer because p is odd.)

Why $x = a^{(p+1)/4}$ works. Because $p \equiv 3 \pmod 4$, $p+1$ is divisible by 4, so $(p+1)/4$ is an integer and x makes sense. Then

$$x^2 = a^{(p+1)/2} = a^{(p-1)/2+1} = a^{(p-1)/2} \cdot a \equiv 1 \cdot a = a \pmod p.$$

Demonstration, $p = 19$, $a = 6$. $(p+1)/4 = 5$, and

$$6^2 \equiv 17, \quad 6^4 \equiv 17^2 = 289 \equiv 4, \quad 6^5 \equiv 4 \cdot 6 = 24 \equiv 5 \pmod{19}.$$

So $x = 5$, and indeed $5^2 = 25 \equiv 6 \pmod{19}$. ✓ The other square root is $-5 \equiv 14$. (Also $6^9 \equiv 1$, confirming 6 is a square.)

What goes wrong for $p = 13$, $a = 10$. Here $p \equiv 1 \pmod 4$, so $(p+1)/4 = 14/4 = 7/2$ is *not an integer*: the formula cannot even be written down. The algebra above needed $(p+1)/4 \in \mathbb{Z}$; what it really shows is that $x^2 = a$ requires $x = a^{(p+1)/4}$, an "a to the power $7/2$," which has no meaning modulo 13. If you try the nearest thing, $a^3 = 10^3 = 1000 \equiv 12 \equiv -1 \pmod{13}$, you get $x^2 \equiv 1 \neq 10$. The actual square roots of 10 modulo 13 are 6 and 7 ($6^2 = 36 = 2 \cdot 13 + 10$), but this formula does not find them; primes $\equiv 1 \pmod 4$ need a different (and more complicated) algorithm, as Problem 5 notes.

Problem 2: square roots modulo $n = pq$, given the factorization

Suppose $n = pq$ with $p \equiv q \equiv 3 \pmod 4$, and a is a square modulo n. Then a is also a square modulo p and modulo q (any x with $x^2 \equiv a \pmod n$ works modulo each prime). So:

1. Compute $r_p = a^{(p+1)/4} \bmod p$ and $r_q = a^{(q+1)/4} \bmod q$ using Problem 1. The square roots of a modulo p are $\pm r_p$, and modulo q they are $\pm r_q$.
2. For each of the four sign choices, solve $x \equiv \pm r_p \pmod p$, $x \equiv \pm r_q \pmod q$ by CRT (the moduli are coprime).

Each of the four x satisfies $x^2 \equiv a$ modulo p and modulo q, hence modulo n (by CRT again). So we get all four square roots of a modulo n. Without the factorization, we cannot do step 1.

Problem 3: the four square roots of 71 modulo 77

Modulo 7: $71 \equiv 1 \pmod 7$, whose square roots are ± 1, i.e. 1 and 6. (The formula agrees: $1^{(7+1)/4} = 1^2 = 1$.)

Modulo 11: $71 \equiv 5 \pmod{11}$, and $(11+1)/4 = 3$, so $r = 5^3 = 125 \equiv 4 \pmod{11}$. Check: $4^2 = 16 \equiv 5$. ✓ The square roots are 4 and $-4 \equiv 7$.

Combine with CRT. We need $11^{-1} \pmod 7$ and $7^{-1} \pmod{11}$: $11 \cdot 2 = 22 \equiv 1 \pmod 7$ and $7 \cdot 8 = 56 \equiv 1 \pmod{11}$. So

$$x \equiv r_7 \cdot (11 \cdot 2) + r_{11} \cdot (7 \cdot 8) = 22\, r_7 + 56\, r_{11} \pmod{77}.$$

r_7	r_{11}	$22r_7 + 56r_{11}$	$x \bmod 77$
1	4	246	15
1	7	414	29
6	4	356	48
6	7	524	62

The four square roots of 71 modulo 77 are

$$15,\ 29,\ 48,\ 62 \qquad (= \pm 15,\ \pm 29).$$

Check: $15^2 = 225 = 2 \cdot 77 + 71$ and $29^2 = 841 = 10 \cdot 77 + 71$. ✓

Problem 4: square roots give factoring

Suppose we can find *all* square roots modulo $n = pq$. Pick any a that is a square, and get its four roots $\pm x$, $\pm y$ with $y \not\equiv \pm x$. Then

$$x^2 \equiv y^2 \pmod n \quad \Longrightarrow \quad n \mid (x-y)(x+y),$$

but $n \nmid x - y$ and $n \nmid x + y$ (since $y \not\equiv \pm x$). So the prime factors of n are split between the two factors, and $\gcd(x-y, n)$ is a nontrivial factor of n. This is exactly the "$x^2 \equiv y^2$" principle behind Fermat factoring, the quadratic sieve and Miller-Rabin witnesses.

Example from Problem 3: $x = 15$, $y = 29$ are both square roots of 71 modulo 77, and $\gcd(29 - 15, 77) = \gcd(14, 77) = 7$. Likewise $\gcd(29 + 15, 77) = \gcd(44, 77) = 11$.

(In practice one phrases it with an "oracle": choose a random r, hand the oracle $a = r^2 \bmod n$, and get back some square root x. With probability 1/2 we have $x \not\equiv \pm r$, and then $\gcd(x - r, n)$ factors n; repeat a few times.)

Together with Problem 2, this shows: *factoring n is equivalent to finding square roots modulo n.*

Problem 6: the square root of 3 modulo 11, and why the method works

Here $11 \equiv 3 \pmod 4$ and $(11+1)/4 = 3$. First, $3^{(11-1)/2} = 3^5 = 243 = 22 \cdot 11 + 1 \equiv 1$, so 3 is a square. Then

$$x = 3^3 = 27 \equiv 5 \pmod{11}, \qquad 5^2 = 25 \equiv 3. \checkmark$$

The square roots of 3 modulo 11 are 5 and $-5 \equiv 6$.

The dynamical portrait of powers of 3. Multiplying by 3 sends $1 \to 3 \to 9 \to 5 \to 4 \to 1$, so the powers of 3 form a single 5-cycle (the order of 3 modulo 11 is 5). Label each vertex by its value and its exponent:

$$3^0 = 1 \quad \to \quad 3^1 = 3 \quad \to \quad 3^2 = 9 \quad \to \quad 3^3 = 5 \quad \to \quad 3^4 = 4 \quad \to \quad 3^5 = 1 \text{ (back to the start)}$$

(The other six residues $2, 6, 7, 8, 10$ and 0 are not powers of 3; they would appear on other cycles of the "multiply by 3" portrait.)

Reading the method off the picture. On this cycle, every residue is 3^k with k an exponent *modulo* 5 (the cycle length). *Squaring* a vertex doubles its exponent: $3^k \mapsto 3^{2k}$. Our computed root is the vertex $3^3 = 5$, and squaring it lands on $3^6 = 3^1 = 3$, because $6 \equiv 1 \pmod 5$. So 5 is a square root of 3.

Why does this always work when $p \equiv 3 \pmod 4$? If a is a square, its cycle length L (the order of a) divides $(p-1)/2$, which is *odd*. The formula $x = a^{(p+1)/4}$ has exponent $(p+1)/4$, and squaring doubles it to $(p+1)/2 = (p-1)/2 + 1 \equiv 1 \pmod L$, since $L \mid (p-1)/2$. So in the exponent, "multiply by $(p+1)/2$" is the identity on the cycle: the square of x is $a^1 = a$ itself. (For $p = 11$: $L = 5$ divides $(11-1)/2 = 5$, and $(11+1)/2 = 6 \equiv 1 \pmod 5$.) Equivalently: on a cycle of odd length, doubling the exponent is a permutation, and $(p+1)/4$ is the position that doubling sends to 1. When $p \equiv 1 \pmod 4$, $(p-1)/2$ is even, so the cycle of a can have even length, doubling need not be invertible on it, and this shortcut fails (as in Problem 1).