

1

a.

$$\begin{aligned}366 &= 254 + 112 \\254 &= 2 \cdot 112 + 30 \\112 &= 3 \cdot 30 + 22 \\30 &= 22 + 8 \\22 &= 2 \cdot 8 + 6 \\8 &= 6 + 2 \\6 &= 3 \cdot 2 + 0\end{aligned}$$

Therefore, $\gcd(254, 366) = 2$.

b.

$$\begin{aligned}35 &= 2 \cdot 16 + 3 \\16 &= 5 \cdot 3 + 1\end{aligned}$$

Working backwards tells us that

$$\begin{aligned}1 &= 16 - 5(3) \\&= 16 - 5(35 - 2(16)) = 11(16) - 5(35)\end{aligned}$$

So we find that $L = 11$ and $K = -5$.

c. We actually already have this from part (b), it is just $L = 11$.

d.

$$\begin{aligned}143 &= 84 + 59 \\84 &= 59 + 25 \\59 &= 2 \cdot 25 + 9 \\25 &= 2 \cdot 9 + 7 \\9 &= 7 + 2 \\7 &= 3 \cdot 2 + 1\end{aligned}$$

Again, we work backwards to find

$$\begin{aligned}1 &= 7 - 3(2) \\ &= 7 - 3(9 - 7) = 4(7) - 3(9) \\ &= 4(25 - 2(9)) - 3(9) = 4(25) - 11(9) \\ &= 4(25) - 11(59 - 2(25)) = 26(25) - 11(59) \\ &= 26(84 - 59) - 11(59) = 26(84) - 37(59) \\ &= 26(84) - 37(143 - 84) \\ &= 63(84) - 37(143)\end{aligned}$$

So, $84^{-1} \equiv 63 \pmod{143}$.

2

a. I am not going to show all my steps in this problem, but using the same logic as in problem 1, we find that $a = 19$ and $b = -1$.

b. Here we find that $a = 149$ and $b = -11$.

c. Here, we find $a = 9$ and $b = -1$.

d. Using our answers from (a), (b), and (c), we find that $x = 8(-208) + 2(-1936) + 7(-143) \equiv -6537 \pmod{2288}$. Reducing, we find that $x \equiv 327 \pmod{2288}$.

Alternate solution (note this is just how I learned to do it and some people may find it more intuitive): To start, we write $x = 8 + k \cdot 11$ for some $k \in \mathbb{Z}$. Then $8 + k \cdot 11 \equiv 2 \pmod{13}$, which can be reduced to $k \cdot 11 \equiv 7 \pmod{13}$, $k \equiv 6 \cdot 7 \equiv 3 \pmod{13}$ (because we can easily compute 11^{-1} using the same methods as before). So, $k = 3 + l \cdot 13$, which we plug into our original equation to see that $x = 8 + (3 + l \cdot 13)11 = 8 + 33 + 143 \cdot l = 41 + 143l$. Moving on to our next congruence, we plug in $41 + 143l \equiv 7 \pmod{16}$, or $15l \equiv 14 \pmod{16}$. We compute $15^{-1} \equiv 15 \pmod{16}$ and use this information to see that $l \equiv 15 \cdot 14 \equiv 2 \pmod{16}$. So $l = 2 + m \cdot 16$. Finally, we plug this back into our equation for x to see that

$$\begin{aligned}x &= 41 + 143(2 + m \cdot 16) \\ &= 41 + 286 + 2288m \\ &= 327 + 2288m\end{aligned}$$

Taking $m = 0$ to find our smallest value, we get $x = 327$.

3

a. We can see that, if $n \neq 2$ is prime, we will get to the last line of this algorithm. On the last line, we can see that for a prime n , the only square roots of $r^2 \pmod n$ are $\pm r$. So, the last line will indeed verify that our n is prime. If n is composite and the algorithm stops on either line 2, 3, or 4, we know we are right with probability 1, since it is impossible to satisfy any of these conditions and be prime. If n is composite and reaches the last line, we can consider the worst case scenario. If *SQRT* actually does output a square root and $n = pq$, then we know that there are four square roots and that exactly two of them are $\pm r$. Since four is the fewest number of square roots for a square in a given composite modulus, this really is the worst case. Therefore, in the worst case we have a 50% chance of returning composite, and so our overall probability of getting a composite number right is at least $\frac{1}{2}$.

b. By the definition of a quadratic residue, we know that there exists some x such that $x^2 \equiv a \pmod p$. So $a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$ by Fermat's Little Theorem. Therefore, the fact that a is a quadratic residue tells us that $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. So, $(a^{m+1})^2 = a^{2m+2} = a \cdot a^{2m+1} \equiv a \pmod p$ (because if $x_1 \equiv x_2 \pmod p$ and $x_3 \equiv x_4 \pmod p$ then $x_1 \cdot x_3 \equiv x_2 \cdot x_4 \pmod p$).

c. First, we follow the same first lines as in part (a), that is keep the third and fourth lines of the algorithm (we don't need to check that x is even or equal to 2 because $x \equiv 3 \pmod 4$). For the last line, if $x \equiv 3 \pmod 4$, we know that x is of the form $x = 4m + 3$. We should pick some $r \in \{1, \dots, x - 1\}$. We compute $a \equiv r^2 \pmod x$; if a^{m+1} is a square root of a and $a^{m+1} \equiv \pm r \pmod x$ then we say that x is prime. Otherwise, we say that x is composite. Essentially, we run the algorithm from part a using the sqrt algorithm that we proved was valid in part b. In part a we showed that this algorithm would be a primality test as long as the sqrt algorithm was guaranteed to be successful on primes of the form $4m+3$. In part b, we showed that this algorithm meets that requirement.