Problem 1: The Extended Euclidean GCD Algorithm

a.

\[ 1239 = 735 \cdot 1 + 504 \]
\[ 735 = 504 \cdot 1 + 231 \]
\[ 504 = 231 \cdot 2 + 42 \]
\[ 231 = 42 \cdot 5 + 21 \]
\[ 42 = 21 \cdot 2 + 0 \]

Therefore, \( \text{gcd}(1239, 735) = 21 \).

b.

\[ 62 = 27 \cdot 2 + 8 \]
\[ 27 = 8 \cdot 3 + 3 \]
\[ 8 = 3 \cdot 2 + 2 \]
\[ 3 = 2 \cdot 1 + 1 \]

Working backwards tells us that

\[ 1 = 3 - 1(2) \]
\[ = 3 - 1(8 - 2(3)) = 3(3) - 1(8) \]
\[ = 3(27 - 3(8)) - 1(8) = 3(27) - 10(8) \]
\[ = 3(27) - 10(62 - 2(27)) = 23(27) - 10(62) \]

So we find that \( L = 23 \) and \( K = -10 \).

c. We actually already have this from part (b), it is just \( L \equiv 23 \pmod{62} \).

d.

\[ 1245 = 143 \cdot 8 + 101 \]
\[ 143 = 101 + 42 \]
\[ 101 = 2 \cdot 42 + 17 \]
\[ 42 = 2 \cdot 17 + 8 \]
\[ 17 = 2 \cdot 8 + 1 \]
Again, we work backwards to find

\[
1 = 17 - 1(2 \cdot 8) \\
= 17 - 2(42 - 2(17)) = 5(17) - 2(42) \\
= 5(101 - 2 \cdot 42) - 2(42) = 5(101) - 12(42) \\
= 5(143 - 42) - 12(42) = 5(143) - 17(42) \\
= 5(143) - 17(143 - 101) = -12(143) + 17(101) \\
= -12(143) + 17(1245 - 8 \cdot 143) = -148(143) + 17(1245) \\
\]

So, \(1245^{-1} \equiv 17 \text{ mod } 143\).

**Problem 2: Practice with the Chinese Remainder Theorem**

a. Using the same logic as in problem 1, we find that \(a_1 = 467\) and \(b_1 = -4\).

b. Here, we find that \(a_2 = 206\) and \(b_2 = -13\).

c. Here, we find \(a_3 = 99\) and \(b_3 = -32\).

d. We compute \(n = 7 \cdot 19 \cdot 43 = 5719\), and

\[
c_1 = \frac{n}{7} = 817 \\
c_2 = \frac{n}{19} = 301 \\
c_3 = \frac{n}{43} = 133
\]

Then, using our answers from (a), (b), and (c), we find that

\[
x = 4c_1b_1 + 11c_2b_2 + 5c_3b_3 \\
= 4 \cdot 817 \cdot -4 + 11 \cdot 301 \cdot -13 + 5 \cdot 133 \cdot -32 \\
= -77395 \\
\equiv 2671 \pmod{5719}
\]

**Problem 3: The Blum TDP**

a. *Proof.*

(a) First, let’s assume that \(x\) is a square modulo \(p\). This means that there is some \(y\) such that \(y^2 \equiv x \pmod{p}\). Then

\[
x^{p-1} \equiv (y^2)^{p-1} \pmod{p} \\
\equiv y^{p-1} \pmod{p} \\
\equiv 1 \pmod{p}
\]

by Fermat’s Little Theorem. To show the other direction, consider some \(x\) that is not a square modulo \(p\). Then if \(g\) is some generator of the group, we know we can write \(x\) as
Since \( p \) is a generator means its order is \( p - 1 \), and so \( g^{\frac{p-1}{2}} \) cannot be equal to 1 (mod \( p \)).

(b) Since \( p \equiv 3 \pmod{4} \) we can write \( p = 3 + 4m \), which means that \( p - 1 = 2 + 4m \) and therefore

\[
(-1)^{\frac{p-1}{2}} \equiv (-1)^{2m+1} = -1.
\]

By what we just proved, this implies that \(-1\) cannot be a square mod \( p \).

(c) First, we must show that \( x \) has a square root that is a square. We know that \( x \) is a square and, because \( p \) is prime, it has only two square roots mod \( p \). Let \( y \) be one square root of \( x \), and \( z \) be the other. Because

\[
(-z)^2 \equiv (-1)^2 \cdot z^2 \equiv x \pmod{p},
\]

and because \( z \not\equiv -z \pmod{p} \), we know that \( y = -z \). All we need to do now is show that \( z \) is a square if and only if \( y \) is not a square.

Suppose \( y \) is not a square. Then

\[
z^{\frac{p-1}{2}} \equiv (-y)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \cdot y^{\frac{p-1}{2}} \pmod{p}.
\]

Because \( p \equiv 3 \pmod{4} \), we know that \((-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}\) by what we have shown in part (b). We also know that

\[
(y^{\frac{p-1}{2}})^2 \equiv y^{p-1} \equiv 1 \pmod{p},
\]

so \( y^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p} \). But \( y \) is not a square, so \( y^{\frac{p-1}{2}} \) must equal \(-1\). This means that we have \( z^{\frac{p-1}{2}} \equiv (-1) \cdot (-1) \equiv 1 \pmod{p} \), and so \( z \) is a square.

Suppose \( y \) is a square. Then

\[
z^{\frac{p-1}{2}} \equiv (-y)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \cdot y^{\frac{p-1}{2}} \pmod{p}.
\]

Because \( y \) is a square, and because \( \frac{p-1}{2} \) is odd, we know that \( z^{\frac{p-1}{2}} \equiv (-1) \cdot (1) \equiv -1 \pmod{p} \), and so \( z \) is not a square. Therefore, exactly one of \( y, z \) is a square, and so \( x \) has exactly one square root that is also a square.

We know that \( x^2 \equiv (x \pmod{p})^2 \pmod{p} \), and similarly that \( x^2 \equiv (x \pmod{q})^2 \pmod{q} \). This means that we could use the Chinese Remainder Theorem to reconstruct \( x^2 \pmod{pq} \) from the values \( x^2 \pmod{p} \) and \( x^2 \pmod{q} \). Because the map induced by the CRT is one-to-one, \( x^2 \pmod{pq} \) would be equal to \( y^2 \pmod{pq} \) for some \( y \) if and only if \( x^2 \equiv y^2 \pmod{pq} \) and \( x^2 \equiv y^2 \pmod{q} \). By part 3, we know that if \( x \) and \( y \) are both QRs, then \( x \equiv y \pmod{p} \) and \( x \equiv y \pmod{q} \). This means that \( x \) and \( y \) are the same. So if any two QRs \( x \) and \( y \) map to the same value, then we know that \( x \equiv y \pmod{pq} \). This shows that the function is one-to-one. This means that each value in the domain maps to a unique value of the range. Because this function maps from QRs to QRs, the domain is the range, and so every value in the range must have a value in the domain that produced it. Therefore, \( f_N(x) \) is a permutation.
b. The fact that \( a \) is a quadratic residue tells us that
\[
a^{\frac{p-1}{2}} \equiv a^{2m+1} \equiv 1 \pmod{p}.
\]

It immediately follows that
\[
(a^{m+1})^2 \equiv a^{2m+2} \equiv a \cdot a^{2m+1} \equiv a \pmod{p}.
\]

c. Given some input \( y \), we find a square root of \( y \pmod{p} \) and a square root of \( y \pmod{q} \) using part b. Then we use the CRT to get the square root of \( y \pmod{N} \).

d. We know \( x^2 - y^2 \equiv 0 \pmod{N} \), so \( N \mid (x + y)(x - y) \). \( N \) cannot divide \( x + y \) or \( x - y \) because \( x \not\equiv \pm y \pmod{N} \). Therefore, since \( N = pq \), where \( p \) and \( q \) are prime, one of \( \{p, q\} \) divides \( x + y \) and the other divides \( x - y \), but \( pq \) divides neither. This means that, if we compute \( \gcd(N, x - y) \), it must be either \( p \) or \( q \), which we can of course use to fully factor \( N \).

e. To finish the reduction, if \( y \not\equiv \pm x \), we can use part b. to factor \( N \). If \( y = \pm x \), \( A \) just fails.

Suppose \( A \) has non-negligible probability \( \epsilon \) of breaking the Blum TDP. For a randomly chosen input \( x \leftarrow \mathbb{Z}_N^* \) to \( B \), \( A \)'s input \( x^2 \pmod{N} \) is a random element of \( \mathbb{QR}_N \), so \( A \) will succeed with probability \( \epsilon \). If \( A \) succeeds, \( A \) outputs some square root \( y \) of \( x^2 \). Since \( x^2 \) has four square roots, and \( x \) was chosen randomly from \( \mathbb{Z}_N^* \), the probability that \( x \not\equiv \pm y \pmod{N} \) is \( \frac{1}{4} \). Therefore, if \( A \) succeeds, \( B \) succeeds with probability \( \frac{1}{2} \), so \( B \) succeeds with non-negligible probability \( \frac{\epsilon}{2} \).

**Problem 4: One-Way Functions Under XOR**

Let \( f_1 \) and \( f_2 \) be OWFs with the same-size output. Now consider \( f(x) = f_1(x_1) \oplus f_2(x_2) \), where \( x = x_1 \circ x_2 \) so that \( |x_1| = \lceil \frac{|x|}{2} \rceil \), and \( |x_2| = \lfloor \frac{|x|}{2} \rfloor \), and when XORing strings of unequal length, you can pretend that blank characters at the end of the shorter strings are 0’s.

a. Assuming that length-preserving one-way functions exist, give an example of OWFs \( f_1 \) and an \( f_2 \) such that \( f \) is a OWF, and prove that in this case \( f \) is a OWF. You must also show that your choices of \( f_1 \) and \( f_2 \) are OWFs.

Let \( f' : \{0, 1\}^n \to \{0, 1\}^n \) be a OWF. Then consider \( f_1(x) = f'(x) \circ 0^{|x|} \) and \( f_2(x) = 0^{|x|} \circ f'(x) \).

To see that \( f_1 \) is a OWF, assume that it is not and that \( A \) inverts \( f_1 \) with non-negligible probability \( \nu \). Then we can construct \( B \) to invert \( f' \) as follows: on input \( y \), \( B \) sets \( y' = y \circ 0^{|y|} \), and passes \( y' \) to \( A \). \( B \) then outputs whatever \( A \) outputs.

With probability \( \nu \), \( A \) will return an \( x' \) such that \( f_1(x') = y \circ 0^{|y|} \). But by definition of \( f_1 \), we also have that \( f_1(x') = f'(x') \circ 0^{|y|} \), and so \( y \circ 0^{|y|} = f'(x') \circ 0^{|y|} \Rightarrow f'(x') = y \), which means that with non-negligible probability \( \nu \), \( B \) outputs an \( x' \) such that \( f'(x') = y \).

We can write a similar argument for why \( f_2 \) is a OWF: on input \( y \), \( B \) will construct \( y' = 0^{|y|} \circ y \), pass \( y' \) to \( A \), and output whatever \( A \) outputs. The analysis is analogous to the one for \( f_1 \).
Now we will show that given the above choice of \( f_1 \) and \( f_2 \), \( f \) is a OWF. First, assume that it is not, and that it is inverted by \( A \). We then construct \( B \) to invert \( f' \): on input \( y \), \( B \) sets \( y' = y \circ f'(r) \), where \( r \leftarrow \{0,1\}^{|y|} \). Then \( B \) passes \( y' \) to \( A \). If \( A \) outputs \( x' \), then \( B \) outputs the first half of \( x' \).

With probability \( \nu \), \( A \) will output an \( x' \) such that \( f(x') = y \circ f'(r) \). But by definition of \( f \), we also have that \( f(x') = f_1(x_1') \oplus f_2(x_2') \) (where \( x_1 \circ x_2 = x \)). Given our definitions of \( f_1 \) and \( f_2 \), this gives us:

\[
\begin{align*}
    f(x') & = f_1(x_1') \oplus f_2(x_2') \\
        & = (f'(x_1) \circ 0^{|y|}) \oplus (0^{|y|} \circ f'(x_2)) \\
        & = (f'(x_1) \oplus 0^{|y|}) \circ (f'(x_2) \oplus 0^{|y|}) \\
        & = f'(x_1) \circ f'(x_2)
\end{align*}
\]

So \( A \) outputs an \( x' \) such that \( f(x') = y \circ f'(r) = f'(x_1') \circ f'(x_2') \). But we know that \( f'(r) = f'(x_2') \), which means that \( y = f'(x_1') \). Thus, with probability \( \nu \), \( B \) outputs \( x_1' \) such that \( y = f'(x_1') \).

**b. Assuming that length-preserving one-way functions exist, give an example of OWFs \( f_1 \) and \( f_2 \) such that \( f \) is NOT a OWF, and prove that in this case \( f \) is not a OWF. You must also show that your choices of \( f_1 \) and \( f_2 \) are OWFs.**

Let \( f' : \{0,1\}^n \to \{0,1\}^n \) be a OWF. Then let \( f_1 : \{0,1\}^k \to \{0,1\}^{2k} \) be defined as \( f_1(x) = f'(x_1) \circ (x_1 \oplus x_2) \circ 0^k \), and let \( f_2 : \{0,1\}^k \to \{0,1\}^k \) be defined as \( f_2(x) = (x_1 \oplus x_2) \circ f'(x_1) \circ 0^k \), where \( x_1 \circ x_2 = x \).

To see that \( f_1 \) is a OWF, assume that it is not and that \( A \) inverts \( f_1 \) with non-negligible probability \( \nu \). Then we can construct \( B \) to invert \( f' \) as follows: on input \( y = f'(x) \), where \( y \in \{0,1\}^n \), \( B \) chooses \( r_1, r_2 \leftarrow \{0,1\}^n \), and sets \( y' = y \circ (r_1 \oplus r_2) \circ 0^{2n} \). Then \( B \) passes \( y' \) to \( A \). If \( A \) outputs \( x' \), then \( B \) outputs \( x_1' \), the first half of \( x' \).

With probability \( \nu \), \( A \) will return an \( x' \) such that \( f_1(x') = y' = y \circ (r_1 \oplus r_2) \circ 0^{2n} \). But by definition of \( f_1 \), we also have that \( f_1(x') = f'(x_1') \circ (x_1' \oplus x_2') \circ 0^{2n} \). This means that \( y \circ (r_1 \oplus r_2) \circ 0^{2n} = f'(x_1') \circ (x_1' \oplus x_2') \circ 0^{2n} \), and so \( y = f'(x_1') \). Thus, with non-negligible probability \( \nu \), \( B \) outputs an \( x_1' \) such that \( f'(x_1') = y \).

We can write a similar argument for why \( f_2 \) is a OWF: on input \( y = f'(x) \), where \( y \in \{0,1\}^n \), \( B \) will choose \( r_1, r_2 \leftarrow \{0,1\}^n \), will set \( y' = (r_1 \oplus r_2) \circ y \circ 0^{2n} \), and will pass \( y' \) to \( A \). Again, \( B \) outputs the first half of the \( x' \) that \( A \) outputs. The analysis is analogous to the one given for \( f_2 \).

Now we will show that for the above choice of \( f_1 \) and \( f_2 \), \( f \) is not a OWF. Assume that we have \( y = f(x) \) (where \( x = x_1 \circ x_2 \circ x_3 \circ x_4 \), and \( y \in \{0,1\}^n \)), and we would like to produce \( x' \) such that \( f(x') = y \). First, let’s denote \( f(x) = f(x_1 \circ x_2 \circ x_3 \circ x_4) \) as \( f(x) = w_1 \circ w_2 \circ w_3 \), where \( |w_1| = |w_2| = \frac{n}{4} \) and \( |w_3| = \frac{n}{2} \).

HW 4 – Solutions-5
We then choose $x'_1, x'_3 \leftarrow \{0,1\}^n$. Then set $x'_2 = f'(x'_3) \oplus x'_1 \oplus w_2$, and $x'_4 = f'(x'_1) \oplus x'_3 \oplus w_1$. Now consider $x' = x'_1 \circ x'_2 \circ x'_3 \circ x'_4$:

\[
\begin{align*}
\text{f}(x') &= \text{f}(x'_1 \circ x'_2 \circ x'_3 \circ x'_4) \\
&= \text{f}_1(x'_1 \circ x'_2) \oplus \text{f}_2(x'_3 \circ x'_4) \\
&= f'(x'_1) \circ (x'_1 \oplus x'_2) \circ (x'_3 \oplus x'_4) \circ f'(x'_3) \circ 0^n \\
&= (f'(x'_1) \oplus x'_1 \oplus x'_4) \circ (x'_1 \oplus x'_2 \oplus f'(x'_3)) \circ (0^n \oplus 0^n) \\
&= (f'(x'_1) \oplus x'_3 \oplus f'(x'_3)) \circ (x'_1 \oplus x'_2 \oplus f'(x'_3)) \\
&= (0^n \oplus w_1) \circ (0^n \oplus w_2) \\
&= w_1 \circ w_2
\end{align*}
\]

But then $f(x') = w_1 \circ w_2 = y$, and so we have successfully inverted $f$. Thus, $f$ cannot be an OWF for this choice of $f_1, f_2$. 

HW 4 – Solutions-6