1 [10]. Fix $n \in \mathbb{N}$.
Let $X$ be the set of binary strings of length $2n$, and define an equivalence relation
$s \sim t$ if $s = t$ or $s = \text{"t reversed"}$
e.g. $10010011 \sim 11001001$.
How many equivalence classes are there? Prove a formula in terms of $n$.
**Answer.** Each equivalence class is of the form $\{t, \text{t reversed}\}$, where those might be equal or not. There are $2^{2n}$ words, of which $2^n$ are their own reverses. So there are $2^n$ equivalence classes of size 1, $\frac{2^{2n}-2^n}{2}$ of size 2, for a total of $2^{2n} + 2^n - 1 + 2^n - 1$.

2. Say we try to isomorph the group $\mathbb{Z}_a \times \mathbb{Z}_b$ with a product of groups $\prod_{i=1}^{m} \mathbb{Z}_{n_i}$, where $1 < n_1 \leq n_2 \leq \ldots \leq n_m$. Let $a = \prod_p p^{a_p}$, $b = \prod_p p^{b_p}$ be their prime factorizations.
2a [10]. In terms of the factorizations of $a, b$, what is the smallest possible value of $m$ (the number of groups multiplied)?
**Answer.** If $a = b = 1$ then the only way to do it is with $m = 0$.
If $\gcd(a, b) = 1$ but they’re not both 1, then $\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_{ab}$ by the Chinese Remainder Theorem. Hence the least $m$ is $m = 1$.
Otherwise $\mathbb{Z}_a \times \mathbb{Z}_b$ is not cyclic, i.e. $\mathbb{Z}_a \times \mathbb{Z}_b$ is already tightest, so the least $m$ is 2.
2b [10]. In terms of the factorizations of $a, b$, what is the largest possible value of $m$ (the number of groups multiplied)?
**Answer.** Using CRT we can pull apart $\mathbb{Z}_a \cong \prod_p \mathbb{Z}_{p^{a_p}}$, and $\mathbb{Z}_b$ likewise, but can’t pull them any further apart. So the biggest $m$ is the number of primes dividing $a$ plus the number of primes dividing $b$. (Note that this handles the $a = b = 1$ case correctly!)

3. Let $\mathbb{E} = \mathbb{F}_3[x]/(x^4 + 1)$.
3a [5]. How many elements does $\mathbb{E}$ have?
**Answer.** $3^4$, since it’s a 4-dim vector space over $\mathbb{F}_3$. (I wrote 2s instead of 3s here first, whoops!)
3b [10]. Find a zero divisor in $\mathbb{E}$.
**Answer.** This is only possible if $\mathbb{E}$ isn’t a field, i.e. if $x^4 + 1$ is reducible. Can we factor it with a linear factor? No, because no element of $\mathbb{F}_3$ is a root. So it’s going to have to be a product of quadratics:
\[
x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d)
= x^4 + (a + c)x^3 + (d + ac + b)x^2 + (ad + bc)x + bd
= x^4 + (d - a^2 + b)x^2 + a(d - b)x + bd
\]
so $a = -c$...
To get \( bd = 1 \) with \( b, d \in \mathbb{F}_3 \), we need \( b = d \neq 0 \), so now we have \( x^4 + (2b - a^2) + 1 \). Since \( b \neq 0, 2b \neq 0, \) so \( a \neq 0, \) but then \( a^2 = 1 \) for both elements of \( \mathbb{F}_3 \setminus \{0\} \). So \( b = 2 \). We haven’t figured out what \( a = -c \) actually is, but that’s okay, because there should be two zero divisors. So try \( a = 1 \):

\[
x^4 + 1 = (x^2 + x + 2)(x^2 - x + 2) \quad \checkmark
\]

In \( \mathbb{E} \), the LHS is zero but those two quadratics aren’t.

4 [10]. Let \( m = \prod_p p^{m_p}, n = \prod_p p^{n_p} \) be their prime factorizations, and consider fields \( \mathbb{E} \) with \( \mathbb{F}_{7^m} \supseteq \mathbb{E} \supseteq \mathbb{F}_{7^n} \).

In terms of \( \{m_p\} \) and \( \{n_p\} \), how many such intermediate fields are there?

**Answer.** The subfields of \( \mathbb{F}_{7^n} \) correspond to the divisors \( j|m \), the \( j \)th one having size \( \mathbb{F}_{7^j} \). It can only contain another subfield \( \mathbb{F}_{7^l} \) if \( n|l \). So we’re counting numbers such that \( j|m \) and \( n|l \).

Let \( j' = j/n \). Then we’re counting \( j' \) dividing \( m/n \). That means that for each prime \( p \) dividing \( m/n \) \( D \) times, our \( j' \) can have \( p \) in it between \( 0 \) and \( D \) times; that’s \( D + 1 \) options.

How many times does \( p \) divide \( m/n \)? Exactly \( m_p - n_p \). So the number of possible \( j' \) (and hence \( j \), and hence intermediate subfields) is \( \prod_p (m_p - n_p + 1) \).

5. Let \( f : X \to Y \) be a one-to-one function, where \( \#X = m, \#Y = n \).

5a [10]. How many functions \( g : Y \to X \) are there such that \( g \circ f : X \to X \) is the identity?

**Answer.** For each of the \( m \) elements \( f(x) \) in the image, we know \( g(f(x)) \); it’s supposed to be \( x \). But for each of the other \( n - m \) elements, we can take them wherever we want in \( X \), and there are \( m \) options. In all, \( m^{n-m} \) possible \( g \). (I wrote \( n^{n-m} \) first... how embarrassing.)

5b [5]. How many functions \( h : Y \to X \) are there such that \( f \circ h : Y \to Y \) is the identity?

**Answer.** Two cases: if \( m = n \) then there’s exactly 1 good \( h \), namely \( h = f^{-1} \).

Otherwise \( m < n \) (since \( f \) was one-to-one) so \( h \) can’t be one-to-one, so \( f \circ h \) can’t be one-to-one, and hence can’t be the identity. We’ve learned that there’s exactly 0 good \( h \).

6 [15]. Let \( x^m - 1, x^n + 1 \in \mathbb{Z}[x] \). Compute their GCD, as a function of \( m, n \).

Your answer should be visibly in \( \mathbb{Z}[x] \); an answer written in \( \mathbb{C}[x] \) will get less credit.

**Answer.** By the fundamental theorem of algebra, we can factor these in \( \mathbb{C}[x] \). So we find the common roots \( \lambda_i \), and then multiply the \( x - \lambda_i \) back together.

If \( x^n = -1 \), then \( x^{2n} = 1 \). But \( x^m = 1 \) also. Let \( g := \gcd(m, 2n) = am + b(2n) \) (using Bézout). Then \( x^g = x^{am+b(2n)} = (x^m)^a(x^{2n})^b = 1 \). Conversely \( x^g = 1 \) implies \( x^m = 1 \) and \( x^{2n} = 1 \), so the \( g \)th roots of unity are the common roots of \( x^m - 1 \) and \( x^{2n} - 1 \).

Put another way, we’re now looking for the GCD of \( x^g - 1 \) and \( x^n + 1 \), where \( g|2n \). Half of the \( 2n \)th roots of unity have \( x^n = -1 \) (the other half have \( x^n = 1 \)). Which of them have \( x^g = 1 \)?

If \( g|n \), then \( x^n = (x^g)^n/g = 1^{n/g} \neq -1 \), so, none. Hence \( \gcd(x^m - 1, x^n + 1) = 1 \). Note that \( g|n \) iff the power of 2 dividing \( n \) is \( \geq \) the power of 2 dividing \( m \).
If \( g \not| n \), but \( g | 2n \), then \( g \) must be even, \( g = 2h \), and \( n/h \) is an odd integer. Now each odd power \( y \) of \( \exp(2\pi i/g) \) (of which there are \( h \)) has \( y^h = -1 \). Then \( y^n = (y^h)^{n/h} = (-1)^{n/h} = -1 \). So we want the \( g \)th roots of unity that aren’t \((g/2)\)th roots, and the gcd is \( (x^g - 1)/(x^{g/2} - 1) = x^{g/2} + 1 \).

Another way to see it: we’re computing

\[
\gcd(x^m - 1, x^n + 1) = \frac{\gcd(x^m - 1, x^{2n} - 1)}{\gcd(x^m - 1, x^n - 1)} = \frac{x^{\gcd(m,2n)} - 1}{x^{\gcd(m,n)} - 1}
\]

7 [15]. Let \( q \) be a prime power, so \( x^3 + 1 = (x + 1)(x^2 - x + 1) \in \mathbb{F}_q[x] \).

Does it factor further? Your answer should depend on \( q \).

(Hint: “Is \(-1\) the only cube root of \(-1\) in \( \mathbb{F}_q \)?”)

**Answer.** Actually the hint only covers most cases; even if \(-1\) is the only cube root, maybe it’s all the roots, \( x^3 + 1 = (x + 1)^3 \). That happens (by the Freshman’s Dream) if \( q \) is a power of 3. So assume it’s not.

Now assume \( 1 \neq -1 \), i.e. \( q \) not a power of 2. By the hint, we’re looking for elements in \( \mathbb{F}_q^\times \) of order 6. This can only happen if \( 6|\#\mathbb{F}_q^\times \), by Lagrange’s theorem; note \( \#\mathbb{F}_q^\times = q - 1 \). Since \( \mathbb{F}_q^\times \) is cyclic (the Primitive Root theorem), it has a \( \mathbb{Z}_6 \) subgroup iff \( 6|\,(q - 1) \). Since \( q \) is odd \( q - 1 \) is even, so one could equivalently write \( 3|\,(q - 1) \).

For example, if \( q = 7 \), then \( 2^3 = 4^3 = 1 \) in \( \mathbb{F}_q \).

Finally, if \( q = 2^m \), then we’re looking for elements in \( \mathbb{F}_q^\times \) of order 3, which happens iff \( 3|(2^m - 1) \), iff \( m \) is even. For example, in \( \mathbb{F}_2[y]/\langle y^2 + y + 1 \rangle \) we have

\[
(x + y)(x + y + 1) = x^2 + x(2y + 1) + y(y + 1) = x^2 + x + 1 = x^2 - x + 1.
\]