Assignment 4
DUE: Thursday, 4/6/2023, work in pairs.

1. Consider the group G_{11}, which (since 11 is prime) is the same as $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ with multiplication mod 11.

    (a) Write down the multiplication table of G_{11}.

    (b) List at least two elements that generate the entire group.

    (c) List at least two elements that generate a proper subgroup of G_{11}, and verify that their order divides the order of the full group.

2. Write down the group multiplication table for G_{24}. What are the inverses of each element?

3. The Euclidean Algorithm amounts to the simple relation $\gcd(a, b) = \gcd(b, a \bmod b)$. By iterating this, the second argument decreases until one reaches 0, in which case the first argument is the gcd. Algorithmically,

```
gcd (a, b)
{
  if b == 0 then
    {
      return a;
    }
  else
    {
      d = gcd(b, a mod b);
      return d;
    }
}
```

   Bézout's Lemma, which is proved, for example, in the document `https://mathcs.clarku.edu/~fgreen/courses/cs201/latexDemo.pdf`, says that for $a, b \in \mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$.

    (a) Show that the Euclidean Algorithm can be extended, given a and b, to determine x and y. Mermin describes this in a very sketchy way in Appendix J (Section J.2). Formalize the algorithm more precisely, either via pseudocode (which can be done by "dressing up" the algorithm given above), or a careful description of the process.

    (b) An immediate consequence of the Extended Euclidean Algorithm is that if $\gcd(a, b) = 1$, we can find $x, y \in \mathbb{Z}$ such that $ax + by = 1$. Show how this leads to an algorithm for determining the inverse of a mod b (or the inverse of b mod a).

4. Let's play RSA! Suppose Bob randomly selects primes $p = 59$, $q = 101$, and coding key $c = 41$. Using c, Alice sends him the encoded message $b = 250$. We, as Bob, want to decode it. You may use a calculator for this problem, for multiplication and modular arithmetic, but try to do as much of it as possible by hand. In particular, trace through the Euclidean Algorithm and its extension, and see how repeated squaring works for powering mod N.

(a) Compute $N = pq$ and[1] $\phi = (p-1)(q-1)$.

(b) Using the Euclidean Algorithm, verify that $c \in G_\phi$, i.e., that $\gcd(c,\phi) = 1$.

(c) Using the extension of the Euclidean Algorithm worked out in Problem 3, compute the inverse of c mod ϕ, i.e., find d such that $cd \equiv 1 \pmod{\phi}$.

(d) Alice sends Bob the message $b = 250$. Decrypt it to determine Alice's original uncoded message a. I.e., via repeated squaring, compute $a = b^d \pmod{N}$.

5. Prove that the Quantum Fourier Transform U_{FT} is unitary. Recall that,

$$\mathsf{U}_{\mathrm{FT}}|x\rangle_n = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i x y}{2^n}} |y\rangle_n.$$

So your task reduces to proving that

$$\mathsf{U}_{\mathrm{FT}}^\dagger \mathsf{U}_{\mathrm{FT}}|x\rangle_n = |x\rangle_n \qquad \text{or} \qquad \mathsf{U}_{\mathrm{FT}}^\dagger \mathsf{U}_{\mathrm{FT}} = 1,$$

for any $0 \le x \le 2^n - 1$.

[1] The notation ϕ is not arbitrary, since it is used for the "Euler totient function," usually denoted ϕ, such that $\phi(n)$ = the number of natural numbers $< n$ that are relatively prime to n.