Solutions to Practice Problems

- Prove that if a_1 and a_2 are units modulo m, then $a_1 a_2$ is a unit modulo m.

  If $b_1 a_1 \equiv 1 \pmod{m}$ and $b_2 a_2 \equiv 1 \pmod{m}$, then $(b_1 b_2)(a_1 a_2) \equiv 1 \pmod{m}$.

- Prove that m is prime if and only if $\phi(m) = m - 1$.

  $\phi(m) = m - 1$ if and only if all the integers between 1 and $m - 1$ are coprime with m if and only if the only divisors of m are 1 and m if and only if m is prime.

- Use FLT to show that 77 is not prime.

  It is enough to find an a coprime with 77 and such that $a^{76} \not\equiv 1 \pmod{77}$. $a = 2$ works.

- Compute all invertible elements modulo 8, i.e. determine $(\mathbb{Z}/8\mathbb{Z})^*$.

  They are the integers in $\{0, 1, 2, 3, 4, 5, 6, 7\}$ coprime with 8, i.e. $1, 3, 5, 7$.

- Prove that $(\mathbb{Z}/8\mathbb{Z})^*$ has no generator. This shows that the Primitive Root Theorem does not necessarily hold for non-prime numbers.

  Suppose g is a generator, i.e. $\{1, 3, 5, 7\} = \{g, g^2, g^3, g^4\}$. Clearly, g is odd. But the square of every odd integer is congruent to 1 modulo 8 and so $g^2 \equiv g^4 \equiv 1 \pmod{8}$, a contradiction.

- (Challenge) Find all positive integers n such that $\phi(n) = 4$.

  Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be the factorization of n into distinct primes $p_1, p_2, \ldots, p_k$. We know that

  $$4 = \phi(n) = \phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_k^{e_k}) = p_1^{e_1 - 1}(p_1 - 1) p_2^{e_2 - 1}(p_2 - 1) \cdots p_k^{e_k - 1}(p_k - 1).$$

  Therefore, $p_i - 1$ is a divisor of 4, for each $1 \leq i \leq k$. But the divisors of 4 are $1, 2, 4$ and so the primes p_i dividing n are either $2, 3$ or 5. In other words, $n = 2^a 3^b 5^c$, for some a, b and c. Using the formula above again it is not difficult to see that the solutions are $n = 5, 8, 10, 12$.