HOMEWORK 5
DUE: 10/29

For reference, consult Chapter 5 and 6 from J&J. Numbered examples/exercises refer to examples/exercises from J&J. For problems which partially or fully appear in J&J, or anywhere else, please do not look at solutions; feel free to look at all other solved problems.

Problem 1. Compute $\phi(n)$ for all $n \leq 16$ (don’t show your work).

Problem 2. Compute the orders of all elements of $(\mathbb{Z}/n)^*$ for the following values of $n$ (don’t show your work): (a) $n = 9$; (b) $n = 10$; (c) $n = 12$.

Problem 3. Suppose $\alpha, \beta \in (\mathbb{Z}/n)^*$.
(a) Show that if $\text{ord}(\alpha)$ and $\text{ord}(\beta)$ are coprime, then $\text{ord}(\alpha \beta) = \text{ord}(\alpha) \text{ord}(\beta)$.
(b) Show that $\text{ord}(\alpha^e) = \frac{\text{ord}(\alpha)}{\gcd(e, \text{ord}(\alpha))}$ for any $e \in \mathbb{N}$.

Problem 4. Let $p$ be a prime. Here’s another proof (due to Gauss) that there is a primitive root mod $p$.
(a) Suppose $p - 1 = q_1^{e_1} \cdots q_k^{e_k}$ is the prime factorization of $p - 1$, where the $q_i$ are distinct primes and the $e_i \in \mathbb{N}$. Show that for each $i$ there is $\alpha_i \in (\mathbb{Z}/p)^*$ with $\alpha_i^{(p-1)/q_i} \not\equiv 1 \mod p$.
(b) Show that $\beta_i = \alpha_i^{(p-1)/q_i} \in (\mathbb{Z}/p)^*$ has order $q_i^{e_i}$.
(c) Show that $\beta = \beta_1 \cdots \beta_k$ is a primitive root mod $p$. (Hint: Use Problem 3(b).)

Problem 5. (cf. §6.6)
(a) Find a primitive root mod 25.
(b) Find all solutions to $x^5 \equiv 1 \mod 275$ (275 = $5^2 \cdot 11$). (Hint: We showed in lecture that 2 was a primitive root mod 11.)

Problem 6. The exponent $e(n)$ of $(\mathbb{Z}/n)^*$ is the smallest $e \in \mathbb{N}$ such that $\alpha^e = 1$ for every $\alpha \in (\mathbb{Z}/n)^*$. For example, $e(15) = 4$.
(a) Show that $e(n) | \phi(n)$, with equality if and only if a primitive root mod $n$ exists.
(b) Show that if $m, n$ are coprime integers, then $e(mn) = \text{lcm}(e(m), e(n))$.
(c) Show that $e(p^e) = \phi(p^e)$ for an odd prime $p$, and $e(2^e) = 1, 2, 2^{e-2}$ depending on whether $e \leq 1, e = 2, e \geq 3$. (Hint: You may use the fact that there is no primitive root mod $2^e$ for $e \geq 3$.)
(d) Compute $e(100)$. What are the last two digits of $2^{550}$?

Here are some additional problems, not to be turned in:

Extra Problem 7. For $n \in \mathbb{N}$, let $f(n)$ be the number of distinct solutions mod $n$ to the equation $x^2 \equiv 1 \mod n$.
(a) What are the solutions to $x^2 \equiv 1 \mod n$ for $n = 2, 4, 8$?
(b) Write the prime factorization of $n$ as $n = 2^e p_1^{e_1} \cdots p_k^{e_k}$ for $p_i$ distinct primes and $e, e_i \geq 0$. Show that $f(n) = 2^{k+\epsilon}$ where $\epsilon$ is 0, 1, or 2 depending on whether $e \leq 1, e = 2$, or $e \geq 3$.
(c) Show that
$$\prod_{0 \leq a < n, \gcd(a, n) = 1} a \equiv \begin{cases} -1 & \text{mod } n \text{ if } f(n) = 2 \\ 1 & \text{mod } n \text{ otherwise} \end{cases}$$
(Hint: Look at our proof of Wilson’s theorem. For $f(n) > 2$, consider the product mod $p_i^{e_i}$.)

Extra Problem 8. Show that $n \in \mathbb{N}$ is a Carmichael number if and only if it is a product of distinct primes, $n = p_1 \cdots p_k$, such that $p_i - 1 | n - 1$ for each $i$. 