Midterm Exam: Due Wednesday, April 11 at the Beginning of Class

- You are free to use the posted course notes (including the algebra notes), the homework solutions, your personal notes, and your previous homework in solving these problems.
- You may not communicate with anybody else (student or otherwise) about the problems on the exam. You may not consult or receive assistance from any source other than those mentioned above.
- Organize your solutions and write them neatly!

Problem 1: (5 points) Let $n \in \mathbb{N}$ with $n \geq 2$. Based on the prime factorization of n, determine the number of solutions to $x^2 = 1$ in $\mathbb{Z}/n\mathbb{Z}$.

Problem 2: (5 points) Let $\alpha, \beta \in \mathbb{Z}[i]$. For each of the following, either prove the result or find a counterexample.
a. If $N(\alpha)$ and $N(\beta)$ are relatively prime in $\mathbb{Z}$, then α and β are relatively prime in $\mathbb{Z}[i]$.
b. If α and β are relatively prime in $\mathbb{Z}[i]$, then $N(\alpha)$ and $N(\beta)$ are relatively prime in $\mathbb{Z}$.

Problem 3: (5 points) Let $p \in \mathbb{Z}$ be a prime with $p \geq 5$ and let $k \in \mathbb{N}^+$. Suppose that g is a primitive root modulo p^k. Show that g^3 is a primitive root modulo p^k if and only if $p \equiv 2 \pmod 3$.

Problem 4: (7 points) Let $p \in \mathbb{N}$ be an odd prime and let $m \in \mathbb{N}^+$.
a. Show that if $p \equiv 1 \pmod{2m}$, then $x^m \equiv -1 \pmod p$ has a solution in $\mathbb{Z}$.
b. Show that the converse to part a is false for arbitrary m by providing a specific counterexample.
c. Suppose that m is a power of 2. Show that the converse to part a is true, i.e. show that if $x^m \equiv -1 \pmod p$ has a solution in $\mathbb{Z}$, then $p \equiv 1 \pmod{2m}$.

Problem 5 (6 points) Suppose that R is a Euclidean domain that is not a field. Show that there exists a nonzero nonunit $d \in R$ such that for all $a \in R$, either $d \mid a$ or there exists $u \in U(R)$ with $d \mid (a + u)$.
Hint: Start by fixing a Euclidean function N on R such that $N(a) \leq N(ab)$ whenever $a, b \in R \backslash \{0\}$. It might help to think about $\mathbb{Z}$.

Problem 6: (6 points) Let R be a PID and let I be a nonzero ideal of R. Show that there are only finitely many ideals J with $I \subseteq J \subseteq R$.
Aside: Using the Correspondence Theorem, it follows that the ring R/I has finitely many ideals.

Problem 7: (6 points) Consider the following generalization of prime ideals. Define an ideal I of a ring R to be *awesome* if whenever $ab \in I$, either $a \in I$ or there exists $n \in \mathbb{N}^+$ with $b^n \in I$. Classify the awesome ideals of $\mathbb{Z}[i]$.