18.781 – Proofs to Know for Midterm I

I've included the accompanying results in our book for each of the theorems. In some cases, the full result is really a combination of results from the text (as listed below) and the best proofs will seamlessly combine them. In other cases, you may assume earlier results proved in class, and I have tried to list those instances below. I'll pick at least one of these (basically at random) for the midterm.

1. The Fundamental Theorem of Arithmetic (1.14 and 1.16 in NZM)
2. Euclid's Proof of Infinitely Many Primes (1.17 in NZM)
3. Euler's Fermat's Little Theorem (Thm 2.8 in NZM)
4. Linear Congruence Theorem (Thms. 2.9 and 2.17 in NZM)
5. The Chinese Remainder Theorem (Thm. 2.18 in NZM)
6. Hensel's Lemma (Thm. 2.23 in NZM)
7. Solutions to $f(x)$ mod p are bounded by $\deg(f)$ (Thm. 2.26 in NZM)
8. $f(x)$ has $\deg(f)$ solutions if and only if it divides $x^p - x$ mod p (Thm. 2.28 in NZM, you may assume the previous result in proving this theorem.)
9. Condition on solutions to $x^n \equiv a$ mod p (Thm. 2.37 in NZM)
10. There exist $\phi(p-1)$ primitive roots mod p (NZM Thm. 2.36 – you may assume elementary facts about the order of an element, e.g. Lemmas 2.33 and 2.34 in NZM)
11. Gauss' Lemma (Thm 3.2 in NZM)