Simple induction proofs

Fundamental Theorem of Arithmetic: know it and be able to prove the existence part.

Statement of division algorithm

Definition of gcd, either the book's or the more usual "largest common divisor."

Know: any common divisor divides the gcd

Euclidean algorithm for gcd and for s, t such that $as + bt = d$.

Know: gcd is the smallest positive integer of the form $as+bt$, and that the numbers of this form are precisely the multiples of d.

Know $(a, b) = 1$ and $a|bc$ implies $a|c$, and proof. Know and explain the special case a is prime.

Know theorem 2.9: $ax + by = c$ has a solution iff $d|c$. If there is a solution there are infinitely many. Know how to express all solutions.

Definition of $a \equiv b$ as "same remainder".

Theorem: $a \equiv b$ iff $m|a - b$.

Theorem 3.2: adding, subtracting, multiplying both sides preserves congruence. Hence, replacing values with congruent values in polynomials preserves value.

Know: Definition of ϕ; ϕ is multiplicative; formula for ϕ.

Know: $a^{\phi(m)} \equiv 1$, and why this implies Fermat's Little Theorem.

Know: $ax \equiv b \pmod{n}$ has a solution iff $(a, n)|b$, and the proof.

Know: Chinese remainder theorem; know how to write an actual solution for two or three simultaneous solutions (as in problem 1 in section 3.3).