

1. (a) (5 pts) Complete this statement of the division algorithm: For any integers a and b , with $b > 0$, there exist

(b) (15 pts) Use the division algorithm to prove the part of Theorem 1.1.4 which states that if I is a nonempty set of integers that is closed under addition and subtraction, then I contains a positive integer b such that $b \mid n$ for all n in I .
2. (10 pts) Find $\gcd(78, 102)$ and write it as a linear combination of 78 and 102.
3. (a) (5 pts) Complete the following definition: The nonzero integers a and b are said to be *relatively prime* if

(b) (10 pts) Prove Proposition 1.2.3 (a), which states that if (a, b, c) are integers such that $b \mid ac$, then $b \mid (a, b) \cdot c$.

(c) (10 pts) Prove or disprove the following statement, for integers $0 < a < b < c$: $\gcd(a + b, c) = 1 \iff \gcd(a - b, c) = 1$.
4. (a) (5 pts) Complete the following statement of part of Theorem 1.3.5:
The congruence $ax \equiv b \pmod{n}$ has a solution if and only if

(b) (5 pts) Give an example of a linear congruence (of the form $ax \equiv b \pmod{n}$) which has no solution. Explain your answer.

(c) (10 pts) Find all solutions to the congruence $21x \equiv 6 \pmod{45}$.
5. (a) (5 pts) Explain what is meant by the notation \mathbf{Z}_n^\times .

(b) (5 pts) Complete this statement of Euler's theorem (which involves powers of congruence classes): If $[a]_n \in \mathbf{Z}_n^\times$, then
6. (15 pts) Choose **either** Part A **or** Part B.

Part A

Let $[a]^n \in \mathbf{Z}_n^\times$. The multiplicative order of $[a]_n$ is the smallest positive integer k such that $[a]_n^k = [1]_n$. Prove that the multiplicative order of $[a]_n$ is a divisor of $\varphi(n)$.

Part B

Prove that if $0 < n < m$, then $2^{2^n} + 1$ and $2^{2^m} + 1$ are relatively prime.