

1. (Definitions, 20 pts) Complete each of the following definitions.

(a) Let a and b be integers, not both zero. A positive integer d is called the **greatest common divisor** of a and b if

(b) The nonzero integers a and b are said to be **relatively prime** if

(c) Let n be a positive integer. Integers a and b are said to be **congruent modulo n** if

(d) The symbol \mathbf{Z}_n^\times denotes the set of

2. (Theorems, 20 pts) Complete the statements of the following theorems.

(a) (**Division algorithm**). For any integers a and b , with $b > 0$, there exist

(b) (**Solution of linear congruences**) Let a, b and $n > 1$ be integers. The congruence $ax \equiv b \pmod{n}$ has a solution if and only if

If there is a solution, how many distinct solutions are there, modulo n ?

(c) State the **Chinese remainder theorem**.

(d) (**Euler's theorem**): Fill in the blank: If $(a, n) = 1$, then _____ $\equiv 1 \pmod{n}$.

Explain all notation that you may have used in answering part (d).

Answer these questions in your bluebook.

3. (20 pts)

(a) Find $\gcd(108, 225)$ and write it as a linear combination of 108 and 225.

(b) Find all solutions of the congruence $42x \equiv 18 \pmod{108}$. Express your answer as congruence classes modulo 108, and check each answer by substituting it into the original congruence.

4. (20 pts)

(a) Verify that \mathbf{Z}_{18}^\times is cyclic by showing that each element of \mathbf{Z}_{18}^\times can be expressed as a power of $[5]_{18}$.

(b) Solve the following system of simultaneous congruences:

$$x \equiv 4 \pmod{6} \quad x \equiv 5 \pmod{7} \quad x \equiv 9 \pmod{11}$$

Hint: Solve the first two, then solve the system given by your answer and the third congruence.

5. (20 pts)

(a) Write out the proof (from the text) of the part of Theorem 1.1.6 which states that the greatest common divisor of two integers a and b can be expressed as a linear combination of a and b .

(b) Write out the proof (from the text) of Euclid's theorem, which states that there are infinitely many prime numbers.