1 Problems from last week

1. Let \( p \) be a prime number. Prove that \((p-1)! \equiv -1 \pmod{p}\).

2. If \( a \) and \( b \) are positive integers with \( a \equiv b \pmod{n} \), show that \( a^n \equiv b^n \pmod{n^2} \).

3. Prove that for all positive integers \( a > 1 \) and \( n \), \( n \) is a divisor of \( \varphi(a^n - 1) \).

2 Divisibility

The divisibility relation \( | \), defined on the integers, is given by \( a | b \) if \( b = ka \) for some integer \( k \). Before we try to solve any difficult number theory problem, it is important to become acquainted with some of the basic properties of divisibility:

- On the positive integers, the divisibility relation is reflexive \((a | a)\), antisymmetric \((a | b \text{ and } b | a \implies a = b)\), and transitive \((a | b \text{ and } b | c \implies a | c)\).
- If \( a | b \) and \( a | c \), \( a | ab + \beta c \) for any \( \alpha, \beta \).
- If \( a \) and \( b \) are positive and \( a | b \), then \( a \leq b \).

These are all trivial properties, and being able to apply them effortlessly will greatly improve your ability to solve any problem relating to divisibility.

3 Factoring

Factoring is pretty useful in divisibility problems. If \( P(n) \) can be factored into \( Q(n)R(n) \) (where \( Q, R \) are polynomials with integer coefficients), then \( Q(n) | P(n) \) for all \( n \). In particular, \( a - 1 | a^n - 1 \) for all positive integers \( a, n \) with \( a \neq 1 \), and \( a + 1 | a^n + 1 \) for all positive integers \( a, n \) with \( a \neq 1 \) and \( n \) odd.

4 Greatest Common Divisors

Let \( a, b \) be integers. Then the greatest common divisor of \( a \) and \( b \), written as \( \gcd(a, b) \), is the largest integer which is a divisor of both \( a \) and \( b \). Bzout’s identity states that for all \( a, b \), there are integers \( \alpha, \beta \) with \( \alpha a + \beta b = \gcd(a, b) \). (Note, in particular, that an integer can be written in the form \( \alpha a + \beta b \) for some integers \( \alpha, \beta \) iff it is a multiple of \( \gcd(a, b) \).) Additionally, \( \gcd(a, b) = a \) iff \( a | b \).

5 A Criterion

Let \( v_p(n) \), where \( p \) is a prime, be the \( p \)-adic valuation of \( n \); that is, the exponent of \( p \) in the prime factorization of \( n \). Then, \( m | n \) if and only if \( v_p(m) \leq v_p(n) \) for all primes \( p \). Additionally, \( v_p(mn) = v_p(m) + v_p(n) \) for all \( p, m, n \) with \( p \) prime.
6 Problems

1. Prove that \( v_p(\gcd(m, n)) = \min\{v_p(m), v_p(n)\} \) for all \( m, n, p \) with \( p \) prime.

2. Prove that if \( a|m \) and \( a|n \), then \( a|\gcd(m, n) \).

3. Prove that if \( S \) is a nonempty set of integers such that
   
   - for any \( a \) in \( S \), \(-a\) is in \( S \)
   - for any \( a, b \) (not necessarily distinct) in \( S \), \( a + b \) is in \( S \)

   then there is some integer \( n \) such that \( S \) is the set of all multiples of \( n \).

4. Let \( n \) have the prime factorization \( p_1^{e_1}p_2^{e_2} \cdots p_n^{e_n} \). How many divisors does \( n \) have? What is their sum?

5. An multiplicative number-theoretic function \( f \) is a function taking positive integers to positive integers which satisfies \( f(mn) = f(m)f(n) \) for all \( m, n \) with \( \gcd(m, n) = 1 \). Prove that if \( f(n) \) is a multiplicative function, then the function \( g(n) = \sum_{d|n} f(d) \) is multiplicative.

7 More Problems

Modular arithmetic, in addition to the properties of divisibility outlined in this handout, will be useful in solving these problems.

6. Let \( n \) be a positive integer. Prove that the fraction \( \frac{21n + 4}{14n + 3} \) cannot be reduced.

7. Find the largest positive integer \( n \) such that \( n^3 + 100 \) is divisible by \( n + 10 \).

8. Let \( a \) and \( b \) be relatively prime. Prove that \( ab - a - b \) is the largest integer which cannot be expressed as \( ax + by \) where \( x \) and \( y \) are nonnegative integers.

9. Let \( n \) be a positive integer, and let \( a_1, a_2, \ldots, a_k \) be positive integers, all less than \( n \), such that \( \text{lcm}(a_i, a_j) > m \) for all distinct \( i, j \). Prove that

\[
\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_k} < 2.
\]

10. Prove that for every positive integer \( n \geq 2 \), there is a set \( S \) of \( n \) integers such that \((a - b)^2|ab\) for all distinct \( a, b \) in \( S \).