

Assignment I

Topic: Number Theory

1. Let $\{n_i\}_{i=1}^k$ be a pairwise relatively prime family of positive integers. Let $a_1, \dots, a_k$ and $b_1, \dots, b_k$ be integers and set $d_i := \gcd(a_i, n_i)$ for $i = 1, \dots, k$. Show that there exists integer z such that $a_i z \equiv b_i \pmod{n_i}$ for $i = 1, \dots, k$ if and only if $d_i | b_i$ for $i = 1, \dots, k$.
2. For each prime p , let ν_p is a function that maps an integer n to a non-negative integer e such that $n = p^e m$ such that p does not divide m . Let $p_1, \dots, p_r$ be distinct primes, $a_1, \dots, a_r$ arbitrary integers and $e_1, \dots, e_r$ be arbitrary non-negative integers. Show that there exists an integer a such that $\nu_{p_i}(a - a_i) = e_i$ for $i = 1, \dots, r$.
3. Suppose n_1 and n_2 are positive integers and $d = \gcd(n_1, n_2)$. Let a_1, a_2 be arbitrary integers. Show that there exists an integer a such that $a \equiv a_1 \pmod{n_1}$ and $a \equiv a_2 \pmod{n_2}$ if and only if $a_1 \equiv a_2 \pmod{d}$.
4. Let p be an odd prime. Prove that $\sum_{\beta \in \mathbb{Z}_p^*} \beta^{-1} = \sum_{\beta \in \mathbb{Z}_p^*} \beta = 0$.
5. Let p be an odd prime. Show that the numerator of $\sum_{i=1}^{p-1} 1/i$ is divisible by p .
6. Show that if n is divisible by r distinct odd primes, then 2^r divides $\phi(n)$.
7. Let $\phi_2(n)$ defined to be the number of integers $a \in \{0, 1, \dots, n-1\}$ such that $\gcd(a, n) = \gcd(a+1, n) = 1$. Show that if $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, then $\phi_2(n) = n \prod_{i=1}^r (1 - 2/p_i)$.
8. Show that for every positive integer n and for every $\alpha \in \mathbb{Z}_n$, $\alpha^n = \alpha^{n-\phi(n)}$.
9. Prove that for all primes p and integers a , we have $(a+1)^p \equiv a^p + 1 \pmod{p}$. Using this result, prove the Fermat's little theorem.
10. If $N = pq$ and $ed = 1 \pmod{\phi(N)}$, then show that for all $x \in \mathbb{Z}_N$, $(x^e)^d = x \pmod{N}$.