Survey HW 4

nxr8dq, Sankapla Banjade

September 2023

1 Introduction

Problems: 9.2.1 , 9.3.2 , 10.0.1

Let $a, b, c \in \mathbf{Z}$ be integers, and suppose that $a$and$c$ are coprime and that b and c are coprime. Then ab and c are coprime.
By bezouts lemma u say that there exists integers au + cv = gcd (a,c) = 1
By bezouts lemma u say that there exists integers bu‘ + cv‘ = gcd(b,c) = 1
Multiplying gcd(a,c) with gcd(b,c) you get gcd(ab,c)
(au+cv)(bu‘+cv‘) = 1 =gcd(ab,c)
aubu‘ + cv‘au + cvbu + cvcv‘ = 1 = gcd(ab,c)
ab(uu‘) + c(v‘au+vbu + vcv‘) = 1 = gcd(ab,c)
Since the gcd(ab,c) is 1 then ab and c are coprime.

Solve the following
$x \equiv 2 \pmod 5$
$x \equiv 3 \pmod 6$
$x \equiv 4 \pmod 7$
Directions utilise euclidean division algorithm to get GCD.
$x = 2 \pmod 5$
$x = 2 + 5k$ Definition of Congruence
$2 + 5k \equiv 3 \pmod 6$
$5k \equiv 1 \pmod 6$
$5k = 25 \pmod 6$
$k = 5 \pmod 6$
$k = 5 + 6l$
$27 + 30l \equiv 4 \pmod 7$
$30l \equiv -23 \pmod 7$
$30l \equiv 180 \pmod 7$
$l \equiv 6 \pmod 7$
$l = 6 + 7t$
Substitute l into k
$k = 5 + 6(6 + 7t)$ Substitute k into x
$x = 2 + 5(5 + 6(6 + 7t))$
$x = 2 + 5(41 + 42t)$

$$x = 2 + 205 + 210t$$
$$x = 207 + 210t \text{ for } t \in \mathbf{Z}$$

Fix $s \in \mathbf{Z}$ with gcd(s,n) = 1. Prove that $s^{cd} \equiv s \pmod{n}$ Hint: First, reduce to showing if: p,q does not — s then $s^{(p-1)(q-1)} \equiv 1 \pmod{pq}$