# HW 3 Discrete

Bayard Walsh

October 24, 2022

## 1 Euclidean Algorithm Warm-Up

gcd(435, 667) = gcd(667, 435 mod 667)
gcd(667, 435 mod 667) = gcd(667, 435)
gcd(667, 435) = gcd(435, 667 mod 435)
gcd(435, 667 mod 435) = gcd(435, 232)
gcd(435, 232) = gcd(232, 435 mod 232)
gcd(232, 435 mod 232) = gcd(232, 203)
gcd(232, 203) = gcd(203, 232 mod 203)
gcd(203, 232 mod 203) = gcd(203, 29)
gcd(203, 29) = gcd(29, 203 mod 29)
gcd(29, 203 mod 29) = gcd(29, 0)
gcd(29,0) = 29, as b=0 (by Euclidean Algorithm)
Therefore, **gcd(435, 667)= 29**

## 2 Modular Arithmetic Warm-Up

A) Find an inverse of 7 modulo 11.

**8 is an inverse of 7 modulo 11**, as $8 * 7 = 56$ and $56 \equiv_{11} 1$
Found answer by looking for multiples of 7 that are 1 greater than 11 * N, where N is any integer. $5 * 11 = 55$ and $8 * 7 = 56$, which is 1 greater.

B) Find an integer x such that $7x \equiv_{11} 10$.
**x=3**
$7 * 3 = 21$ and $21 \equiv_{11} 10$
Found answer by looking for multiples of 7 that are 10 greater than N * 11, where N is any integer.

C) Which elements of $\{1, 2 \dots 20\}$ are invertible modulo 21?
**Invertible elements=** $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$
Multiples of 21= $\{1, 3, 7, 21\}$
To be invertible with respect to modulo 21, gcd(N,21) = 1
Therefore remove numbers in the set where $gcd(N, 21) \neq 1$
gcd(3,21), gcd(6,21), gcd(9,21), gcd(12,21), gcd(15,21), gcd(18,21) = 3
gcd(7,21), gcd(14,21) = 7

# 3 Greatest Common Divisors

For each of the following statements, either prove that it holds for all integers a, b not both zero, or find a counterexample.

a) $gcd(a, b) = gcd(a + b, ab)$
Counterexample: a=3, b=6
gcd(3,6)=3
gcd(9,18)=9
**Therefore** $gcd(a, b) \neq gcd(a + b, ab)$

b) If $gcd(a, b) = d$ , then $gcd(a/d, b/d) = 1$.
Because $gcd(a, b) = d$, there must exist some integers $n$ and $m$, where $n = a/d$ and $m = b/d$.
Let $a = nd$ and $b = md$
Therefore, $gcd(a/d, b/d) = gcd(nd/d, md/d)$
By definition of the gcd, $d$ contains all factors that $a$ and $b$ have in common.
As $n = a/d$ and $m = b/d$, $n$ and $m$ must be relatively prime, meaning that $gcd(n, m) = 1$
**Therefore,** $gcd(a/d, b/d) = 1$**.**

c) For all integers $c$, if $c|ab$ and $gcd(a, b) = 1$, then $c|a$ or $c|b$.
Counterexample: $a = 4, b = 7, c = 28$
$28|(4 * 7)$ is true and $gcd(4, 7) = 1$
Neither $28|4$ or $28|7$ are true
**Therefore, if** $c|ab$ **and** $gcd(a, b) = 1$**, then** $c|a$ **or** $c|b$ **is not true.**

## 4 Congruence Confluence

a) If $k|n$ and $a \equiv b \pmod{n}$ , then $a \equiv b \pmod{k}$

Let $n, k$ be some positive integers and let $a, b$ be some integers
Assume that $k|n$ and $a \equiv b \pmod{n}$
If $k|n$, by definition of divisibility there must exist some integer $d$ such that $k * d = n$
If $a \equiv b \pmod{n}$, then $n|(a-b)$
Therefore $kd|(a-b)$
As $n, k$ are positive numbers, and $k * d = n$, then $d \neq 0$
As $d$ is a non-zero integer and $kd|(a-b)$, then $k|(a-b)$
If $k|(a-b)$, by the definition of congruent, $a \equiv b \pmod{k}$
**Therefore, if $k|n$ and $a \equiv b \pmod{n}$ , then $a \equiv b \pmod{k}$**

b) If $k|n$ and $a \equiv b \pmod{k}$ , then $a \equiv b \pmod{n}$

Counterexample: let $k = 3, n = 15, a = 10, b = 7$
Therefore, $3|15$ and $10 \equiv 7 \pmod{3}$ are true.
However this would imply $10 \equiv 7 \pmod{15}$, which is not true
**Therefore the statement is false**

c) If $a \equiv b \pmod{n}$ and $a \equiv b \pmod{k}$, then $a \equiv b \pmod{kn}$
Counterexample: let $k = 9, n = 3, a = 12, b = 3$
As $12 \equiv 3 \pmod{3}$ and $12 \equiv 3 \pmod{9}$, conditions are true
However, $12 \equiv 3 \pmod{3 * 9}$ is not true
$27|9$ is false, as no integer n exists such that $27 * n = 9$
**Therefore the proof is false**

# 5 Primes

a) For all primes $p$ and all integers $a, b$, if $a$ and $b$ are both invertible modulo $p$, then $ab$ is invertible modulo $p$.

If $a$ is invertible modulo $p$, then $gcd(a,p) = 1$, by Theorem 9.7
If $b$ is invertible modulo $p$, then $gcd(b,p) = 1$, by Theorem 9.7
If $gcd(a,p) = 1$, then $p \not| a$
If $gcd(b,p) = 1$, then $p \not| b$
Consider Euclids Lemma, as $p$ is prime and $a, b$ are integers such that $p|ab$ then $p|a$ or $p|b$
As $p \not| b$ and $p \not| a$ then $p \not| ab$, because of the contra positive of Euclids Lemma.
Let d be an integer such that $gcd(ab,p) = d$.
As $p$ is prime, $d$ must be 1 or $ab$
However, as $p \not| ab$, $d \neq ab$
Therefore, $d = 1$, and $gcd(ab,p) = 1$
If $gcd(ab,p) = 1$, then $ab$ is invertible modulo $p$.

b) For all primes $p$, $(p-2)! \equiv 1 \pmod p$.

Let $p$ be a prime number, then by Wilson's Theorem, for all primes $p$, $(p-1)! \equiv -1 \pmod p$
Let $(p-1)! = (p-1) * (p-2)!$, by definition of a factorial function
Let $(p-1) * (p-2)! = (p * (p-2)!) + (-1 * (p-2)!)$
Therefore, $p(p-2)! - (p-2)! \equiv -1 \pmod p$
Reduce to $-(p-2)! \equiv -1 \pmod p$ (by modular rules)
Therefore $(p-2)! \equiv 1 \pmod p$

# 6 Contributor List

Hunter Smith, Grey Sign, Nafis Khan