

# Homework 5

Cameron Dart

Math 348

February 25, 2016

**Question 6.8.** Compute gcd of (126,224) and (221,299).

$$\gcd(126, 224) = \gcd(126, 98) \tag{1}$$

$$= \gcd(28, 98) \tag{2}$$

$$= \gcd(28, 14) \tag{3}$$

$$= 14 \tag{4}$$

(5)

$$(126)(4) + (224)(-7) = 14 \tag{6}$$

$$896 - 882 = 14 \tag{7}$$

$$14 = 14 \tag{8}$$

$$\gcd(221, 299) = \gcd(221, 78) \tag{9}$$

$$= \gcd(65, 78) \tag{10}$$

$$= \gcd(65, 13) \tag{11}$$

$$= 13 \tag{12}$$

(13)

$$(221)(-4) + (299)(3) = 13 \tag{14}$$

$$-884 + 897 = 13 \tag{15}$$

$$13 = 13 \tag{16}$$

(17)

**Question 6.9.** Find all solutions for the diophantine equations.

a)  $17x + 13y = 200$

1.  $\gcd(17, 13) = 1, 1|200 \therefore$  a solution exists.
2.  $17x + 13y = 1$ 
  3. let  $x = -3, y = 4$
  4.  $17(-3) + 13(4) = 1$
  5.  $1 = 1$
6. soln:  $(x, y) = 200 * (-3, 4)$ 
  7. soln:  $(x, y) = (-600, 800)$
8. let S be the set of solutions to the diophantine equation.
9.  $S = \{(-600 + 15k, 800 + 17k), k \in \mathbb{Z}\}$

**b)**  $21x + 15y = 93$

1.  $\gcd(21, 15) = 3, 3|93 \therefore$  a solution exists.
2.  $\frac{21x+15y=93}{3}$
3.  $7x + 5y = 31$ 
  4.  $7x + 5y = 1$
  5. let  $x = 3, y = -4$
  6. soln:  $(x, y) = 31 * (3, -4)$
  7. soln:  $(x, y) = (93, -124)$
8. let S be the set of solutions to the diophantine equation.
9.  $S = \{(93 + 5k, -124 - 7k), k \in \mathbb{Z}\}$

**c)**  $60x + 42y = 104$

1.  $\gcd(60, 42) = 6, 6 \nmid 104 \therefore$  no integer solution exists.

**d)**  $588x + 231y = 63$

1.  $\gcd(588, 231) = 21$  ,  $21|63 \therefore$  a solution exists
2.  $\frac{588x+231y=63}{21}$
3.  $28x + 11y = 3$
4.  $28x + 11y = 1$
5. let  $x = 2, y = -5$
6. soln  $(x,y)=3 * (2, -5)$
7. soln  $(x,y)=(6, -15)$
8. let  $S$  be set of solutions to the diophantine equation.
9.  $S = \{(6 + 11k, -15 - 28k), k \in \mathbb{Z}\}$

**Question 6.17.** *Proof.*  $\gcd(a+b, a-b) = \gcd(2a, a-b) = \gcd(a+b, 2b)$   $\square$

**Question 6.18.** Suppose  $\gcd(a, b) = 1$ .

*Proof.*  $\gcd(a^2, b^2) = 1$

1.  $\gcd(a, b) = 1 \implies (\exists x, y \in \mathbb{Z}) (ax + by = 1)$  (Integer Combination)
2.  $(ax + by)^3 = 1^3$  (Cube both sides)
3.  $a^3x^3 + 3a^2x^2by + 3ab^2xy^2 + b^3y^3 = 1$  (Expand)
4.  $a^2(x^3 + 3x^2by) + b^2(3axy + by^3)$  (Factor)
5. Let  $m = (x^3 + 3x^2by)$ ,  $n = (3axy + by^3)$  (Declare Vars)
6.  $a^2m + b^2n = 1$  (Substitute back in)
7.  $\gcd(a^2, b^2) = 1$  (Definition of GCD)

$\square$

*Proof.*  $\gcd(a, 2b) \neq 1$

I will prove that  $\gcd(a, b) = 1 \not\Rightarrow \gcd(a, 2b) = 1$  using contradiction.

First, assume  $(\forall a, b \in \mathbb{Z} \neq 0)(\gcd(a, b) = 1 \wedge \gcd(a, 2b) = 1)$ . In other words that both  $(a, b) \wedge (a, 2b)$  respectively are relatively prime.

So  $\gcd(a, b) = 1 \Rightarrow \gcd(a, 2b) = 1$

1.  $\gcd(a, b) = 1$  (Given)
2. Assume  $\gcd(a, 2b) = 1$  (Assumption)
3. Let  $a = 2, b = 5$  (Specify Individual Case)
4.  $\gcd(2, 5) = 1 \therefore a, b$  are relatively prime. (Compute gcd)
5. Now let's consider  $\gcd(a, 2b) = 1$  (Assumption)
6.  $\gcd(2, 2 * 5) = 1$  (Multiplication)
7.  $\gcd(2, 10) = 2 \neq 1$  (Compute gcd)

This contradicts our original assumption  $(\forall a, b \in \mathbb{Z} \neq 0)(\gcd(a, b) = 1 \wedge \gcd(a, 2b) = 1)$

Hence it must be true that  $\gcd(a, b) \not\Rightarrow \gcd(a, 2b) = 1$

□

**Question 6.28.** Suppose that  $\gcd(a, b) = 1, a|n, b|n$ .

*Proof.*  $ab|n$

1.  $a|n, b|n$  (Given)
2.  $(\exists m, n)(c = am, c = bn)$  (Definition of divides)
3.  $\gcd(a, b) = 1 \therefore a, b$  are *relatively prime* (Given)
4.  $\exists s, t \in \mathbb{Z}$  such that,  $as + bt = 1$  (Integer Combination of  $a, b$ )
5.  $c(as + bt) = c$  (Multiply both sides by  $c$ )
6.  $cas + cbt = c$  (Distributive Property of Multiplication)
7.  $(bn)as + (am)bt = c$  (Substitutions from 2)
8.  $ab(ns + mt) = c$  (Factor out  $ab$ )
9. Let  $u = ns, v = mt, z = (u + v)$  (Reassign Variables)
10.  $ab(u + v) = c$  (Rewrite  $u = ns, v = mt$ )

11.  $abz = c$  (Rewrite  $z = (u + v)$ )

12.  $ab|c$  (Definition of Divides)

As shown through a direct proof, if  $\gcd(a, b) = 1 \wedge a|n \wedge b|n \implies ab|n$   $\square$