

## Problem Set #2

### 1 Order on $\mathbb{Z}$

#### Exercise 1 :

Prove that in any unitary commutative ordered ring  $R$ , for any  $x, y \in R$  :

1.  $x > y \Rightarrow x + c > y + c$ , for all  $c \in R$ .
2.  $x \neq 0 \Rightarrow x^2 > 0$ .
3. If  $a > 0$  and  $b > 0$  then  $a > b \Leftrightarrow a^2 > b^2$ . (Hint :  $(b^2 - a^2) = (b - a)(b + a)$ . Use Rule of Signs).

#### Solution :

1.  $x > y \Rightarrow x - y > 0$ . But

$$\begin{aligned}x - y &= x + (-y) = x + 0 + (-y) \\&= x + [c + (-c)] + (-y) \\&= (x + c) + [(-y) + (-c)] = x + c + (-(y + c)) \\&= (x + c) - (y + c)\end{aligned}$$

so  $x > y \Leftrightarrow (x + c) - (y + c) > 0 \Leftrightarrow x + c > y + c$ .

2.  $x$  is either  $> 0$  or  $< 0$ . If  $x > 0$ , then we also have  $x^2 > 0$ . If  $x < 0$ , then  $-x = (-1) \cdot x$  is  $> 0$  and  $(-x)^2 > 0$ . But  $(-x)^2 = (-1)^2 x^2 = x^2$ , so  $x^2 > 0$  in this case too.
3.  $a^2 - b^2 = (a + b)(a - b)$  by distributive laws. Since  $a, b > 0$  are automatically have  $a + b > 0$  and by the rules of signs,  $(a + b)(a - b) > 0 \Leftrightarrow (a - b) > 0$ . Thus  $a^2 > b^2 \Leftrightarrow a^2 - b^2 > 0 \Leftrightarrow (a + b)(a - b) > 0 \Leftrightarrow a - b > 0 \Leftrightarrow a > b$ , if  $a$  and  $b$  are  $> 0$ .

### 2 Equivalence relation on sets

#### Exercise 2 :

For  $n > 1$  define  $a \equiv b \pmod{n}$  to mean

$b - a$  is an integer multiple of  $n$

Verify that this is an RST relation on  $X = \mathbb{Z}$ .

#### Solution :

1. Reflexive :  $a \sim_R a$ . Proof :  $(a - a) = 0 \cdot 5$  is a multiple of 5 ;

2. Symmetric :  $a \sim_R b \Rightarrow b \sim_R a$ . Proof : If  $b - a = 5k$  for some  $k \in \mathbb{Z}$  then  $a - b = (-1) \cdot k = 5 \cdot (-k)$  is also an integer multiple of 5.
3. Transitive :  $(a \sim_R b)$  and  $(b \sim_R c) \Rightarrow (a \sim_R c)$ . Proof : By hypotheses,  $\exists k, l \in \mathbb{Z}_+$  such that  $b = a + 5k$ ,  $c = b + 5l$ . Then  $c = b + 5l = (a + 5k) + 5l = a + 5(k + l) \Rightarrow c - a =$  multiple of 5  $\Rightarrow c \sim_R a$ .

### 3 Induction

#### Exercise 3 :

Prove  $n^2 = (\text{sum of first } n \text{ odd integers}) = \sum_{k=1}^n (2k - 1) = 1 + 3 + \cdots + (2n - 1)$ .

**Solution** : By induction : certainly true if  $n = 1$ . If true at level  $n$ , then at level  $n + 1$  we have

$$(\text{sum}) = (1 + 3 + \cdots + 2n - 1) + (2(n + 1) - 1) = n^2 + 2n + 2 - 1 = n^2 + 2n + 1 = (n + 1)^2$$

So  $(P(n) \text{ true}) \Rightarrow (P(n + 1) \text{ true})$ .  $P(n)$  is true for all  $n \in \mathbb{N}$ .

### 4 Integers

#### 4.1 Absolute value

##### Exercise 4 :

Prove

$$|x + y| \leq |x| + |y|$$

in any commutative ordered ring  $R$ .

##### **Solution** :

Since  $x^2 \geq 0$  for every  $x \in R$ ,  $|x^2| = x^2 = |x|^2$ . Thus

$$0 \leq |x \pm y|^2 = (x \pm y)^2 = x^2 \pm 2xy + y^2, \text{ for all } x, y \in R$$

Now,  $\pm 2xy \leq 2|xy| = 2|x| \cdot |y|$ , because  $u \leq |u|$  for every  $u \in R$ . Hence,

$$|x \pm y|^2 = x^2 \pm 2xy + y^2 \leq x^2 + 2|x| \cdot |y| + y^2 = |x|^2 + 2|x| \cdot |y| + |y|^2 = (|x| + |y|)^2$$

Since  $|x \pm y| \geq 0$ , removing the exponent imply  $|x \pm y| \leq |x| + |y|$ .

#### 4.2 Divisibility in the system of integers

##### 4.2.1 GCD

##### Exercise 5 :

1. Prove  $\gcd(a, b) = \gcd(b, a)$  for  $a, b \neq 0$ .
2. If  $k \in \mathbb{Z}$  is fixed and  $a, b \neq 0$  prove that  $\gcd(a, b) = \gcd(a + kb, b)$ .

3. If  $a, b > 0$  and  $a$  divides  $b$ , show that  $\gcd(a, b) = a$ .

**Solution :**

1. Obviously,  $\mathbb{Z}a + \mathbb{Z}b = \{ra + sb : r, s \in \mathbb{Z}\} = \mathbb{Z}b + \mathbb{Z}a$ . The smallest positive element in this set is equal to  $\gcd(a, b)$  and  $\gcd(b, a)$ .
2.  $\gcd(a + kb, b)$  is the smallest positive element in

$$\Gamma = \mathbb{Z}(a + kb) + \mathbb{Z}b = \{(ra + rkb) + sb : r, s \in \mathbb{Z}\} = \{ra + (rk + s)b : r, s \in \mathbb{Z}\}$$

But as  $s$  runs through  $\mathbb{Z}$ ,  $s' = rk + s$  runs through all of  $\mathbb{Z}$ . Thus

$$\Gamma = \{ra + s'b : r, s' \in \mathbb{Z}\} = \mathbb{Z}a + \mathbb{Z}b$$

We see that  $\gcd(a + kb, b) = \text{smallest positive element in } \Gamma = \gcd(a, b)$ .

Note :  $k$  is fixed. If  $r, s' \in \mathbb{Z}$ , we can get  $ra + (rk + s)b$  to equal  $ra + s'b$  simply by taking  $s = s' - kr$ .

3. All means  $\exists m \in \mathbb{Z}$  such that  $b = ma$ . Then  $\Gamma = \mathbb{Z}a + \mathbb{Z}b$  is  $= \{ra + sb = ra + msa : r, s \in \mathbb{Z}\}$ . This is just the set  $\mathbb{Z}a$  of all multiples of  $a$  : obviously  $ra + msa = (r + ms)a \in \mathbb{Z}a$ , and if  $n \in \mathbb{Z}$ , we can make  $r + ms = n$  in many ways, e.g.  $s = 0$ ,  $r = n$ . Since  $\Gamma = \mathbb{Z}a$ , its smallest positive element is  $1 \cdot a = a$  (every  $n \in \mathbb{N} = \{x \in \mathbb{Z} : x > 0\}$  is  $\geq 1$ ). Thus  $\gcd(a, b) = a$  if  $a|b$ .

**Exercise 6 :**

Taking  $a = 955$ ,  $b = 11422$ , use the extended GCD extended to find first  $\gcd(955, 11422)$  and find  $r, s \in \mathbb{Z}$  such that  $ra + sb = \gcd(955, 11422)$ .

**Solution :**

$$\begin{aligned} 11422 &= 11(955) + 917 \\ 955 &= 1(917) + 38 \\ 917 &= 24(38) + 5 \\ 38 &= 7(5) + 3 \\ 5 &= 1(3) + 2 \\ 3 &= 1(2) + 1 \end{aligned}$$

$$\begin{aligned} \gcd(11422, 955) &= \gcd(917, 955) = \gcd(917, 38) = \gcd(5, 38) = \gcd(5, 3) \\ &= \gcd(2, 3) = \gcd(1, 2) = 1 \end{aligned}$$

To find  $r, s$  such that  $r(955) + s(11422) = \gcd(955, 11422) = 1$  work the calculation displayed above backwards.

$$\begin{aligned} 1 &= 3 - 2 = 3 - (5 - 3) \\ 1 &= -5 + 2 \times 3 = -5 + 2 \times (38 - 7(5)) \\ 1 &= -15(5) + 2(38) = -15(917 - 24(38)) + 2(38) \\ &= -15(917) + 362(38) = -15(917) + 362(955 - 917) \\ &= -377(917) + 362(955) = -377(1142 - 11(955)) + 362(955) \\ &= 377(1142) - 4509(955) \end{aligned}$$

Take  $r = 4509$ ,  $s = -377$ .

**Exercise 7 :**

Generalize the definition of  $\gcd$  to define  $\gcd(a_1, \dots, a_r)$ , where  $a_i$  are nonzero. Make the obvious changes in the definition of  $\gcd(a, b)$  and

1. Prove  $c = \gcd(a_1, \dots, a_r)$  exists by considering the set of integer linear combinations

$$\Gamma = \mathbb{Z}a_1 + \dots + \mathbb{Z}a_r = \left\{ \sum_{i=1}^r k_i a_i : k_i \in \mathbb{Z} \right\}$$

Show that  $\Gamma \cap \mathbb{N} \neq \emptyset$  and verify that the smallest element  $c \in \Gamma \cap \mathbb{N}$  (which exists by the Minimum principle) has a properties required of  $\gcd(a_1, \dots, a_r)$ .

2. Show that  $\Gamma = \mathbb{Z}c$  all integer multiples of  $\gcd(a_1, \dots, a_r)$ .

**Solution :**

1. Given  $a_1, \dots, a_n \neq 0$  define  $\Gamma = \mathbb{Z}a_1 + \dots + \mathbb{Z}a_n$  (set of integer linear combinations). Obviously  $\Gamma \neq \emptyset$  and contains element  $> 0$  (take  $\sum_i m_i a_i$  with  $m_i = 1$ , if  $a_i > 0$ ,  $m_i = -1$  if  $a_i < 0$ ); by the minimum property, there is a (unique) smallest element  $c > 0$  in  $\Gamma \cap \{x \in \mathbb{Z} : x > 0\} = \Gamma \cap \mathbb{N}$ . We claim that  $c$  is a  $\gcd(a_1, \dots, a_n)$  :

(a)  $c > 0$  by definition ;

(b)  $c|a_i$ , all  $i$ .

(c) If  $c'$  divides  $a_1, \dots, a_n$  (say  $a_i = r_i c'$ ) then  $c'$  divides  $c$ .

There is  $m_i \in \mathbb{Z}$  such that  $c = \sum_i m_i a_i$  because  $c \in \Gamma$ . Then  $c = \sum_i (m_i r_i) c'$  so  $c'|c$ .

As in the case  $n = 2$  (Notes) we show that  $c$  divides any element in  $\Gamma$  (obviously each  $a_i \in \Gamma$ ). By Euclidean division algorithm, we may write any  $c' \in \Gamma$  as  $c' = s \cdot c + r$  with  $0 \leq r < c$  and  $s \in \mathbb{Z}$ . Then  $0 \leq r = c' - sc < c$  and  $c' - sc \in \Gamma$ . Since  $c$  is the smallest element in  $\Gamma \cap \mathbb{N}$ , the only possibility is that  $r = 0$ , and then  $c' = sc$ ,  $c|c'$  as required.

2. In the part (b) of (ii), we showed that  $c|c'$  for all  $c' \in \Gamma$ . since  $c \in \Gamma$  too (by definition), and  $k \cdot (\sum_i m_i a_i) = \sum_i (km_i) a_i \in \Gamma$ , for any  $k \in \mathbb{Z}$ ,  $c' = \sum_i m_i a_i \in \Gamma$ , we see that  $\Gamma = \mathbb{Z} \cdot c$ .

**Exercise 8 :**

If  $a, b \neq 0$  and  $u_1, u_2$  are units in  $\mathbb{Z}$ , prove that  $c = \gcd(a, b)$  is equal to  $c' = \gcd(u_1 a, u_2 b)$ .

**Solution :**

Write  $\Gamma = \mathbb{Z}a + \mathbb{Z}b$ ,  $\Gamma' = \mathbb{Z}(u_1 a) + \mathbb{Z}(u_2 b)$ . We know  $\Gamma = \mathbb{Z} \cdot c$  and  $\Gamma' = \mathbb{Z} \cdot c'$ . Write  $c = \gcd(a, b) = r_0 a + s_0 b$ ,  $c' = \gcd(u_1 a, u_2 b) = r_1 (u_1 a) + s_1 (u_2 b)$  ( $r_0, s_0, r_1, s_1 \in \mathbb{Z}$ ) Then  $c' = (r_1 u_1) a + (s_1 u_2) b \in \Gamma$  so  $\Gamma' = \mathbb{Z}c' \subseteq \Gamma$ . Conversely,  $\Gamma = \mathbb{Z} \cdot c$  and  $c = r_0 a + s_0 b$  can be rewritten as  $c = r_0 u_1^{-1} (u_1 a) + s_0 u_2^{-1} (u_2 b) \in \Gamma'$ . Hence  $\Gamma = \mathbb{Z} \cdot c \subseteq \Gamma'$ . Therefore the sets are equal and  $c' = c$ .

#### 4.2.2 Prime factorization

##### Exercise 9 :

Prove that  $p|a \Leftrightarrow p^2|a^2$  for any prime  $p > 1$ .

##### Solution :

$\Rightarrow$  is trivial.  $p|a \Rightarrow \exists m \in \mathbb{Z}$  such that  $a = mp \Rightarrow a^2 = m^2p^2 \Rightarrow p^2|a^2$ .

$\Leftarrow$  The case  $a = 1$  is excluded because we assume  $p > 1$ , which implies  $p^2 > 1$ , and a number  $> 1$  cannot divide  $a = 1$ . In the remaining cases we use unique prime factorization of  $a$ . So, assume  $p > 1$  and  $a > 1$ , suppose  $p^2|a^2$ . Write  $a = \prod_{i=1}^r p_i^{m_i}$  with  $p_i > 1$  distinct prime divisors of  $a$  and multiplicities  $m_i \geq 1$ . Then the unique prime factorization of  $a^2$  must be  $\prod_{i=1}^r p_i^{2m_i}$  (all multiplicities doubled). Now  $p^2|a^2 \Rightarrow p|a^2$  so  $\exists$  index  $i$  such that  $p = p_i$ . But then  $p|a$  desired to prove ( $\Leftarrow$ ). The last part follow from the definition :  $n$  even  $\Leftrightarrow 2|n$ .

##### Exercise 10 :

If  $n = \prod_{i=1}^r q_i$  with each  $q_i > 1$  prime (repeats allowed), and with  $r \geq 2$ , so  $n$  is not already a prime. Show  $\exists$  index  $i$  such that  $q_i \leq \sqrt{n}$ .

**Solution :** Otherwise,  $q_i > \sqrt{n}$  for all  $i$ . Since  $r \geq 2$ , we get  $n \geq q_1 q_2 > \sqrt{n} \sqrt{n} = n$ .

##### Exercise 11 :

If  $p > 1$  a prime and  $n \neq 0$  prove that  $\gcd(p, n) > 1 \Leftrightarrow p$  divides  $n$ .

##### Solution :

( $\Rightarrow$ ) If  $c = \gcd(p, n) > 1$ , we have  $c|p$  so  $p = cm$  for some  $m > 0$  in  $\mathbb{Z}$ . The units  $\pm 1$  in  $\mathbb{Z}$  have absolute value 1 so  $c$  cannot be a unit. By definition of "prime", the other factor must be a unit ( $m = \pm 1$ , hence  $m = 1$ ), otherwise  $p$  would have a nontrivial factorization. Then  $c$  must be  $pm^{-1} = p \cdot 1 = p$  and  $p = c$ . It follows that  $p = c$  also divides  $n$ .

( $\Leftarrow$ ) If  $p$  divides  $n$ ,  $p$  divides  $\gcd(p, n) = c$  (since  $\exists r, s \in \mathbb{Z}$  such that  $c = pr + ns$ ). Thus  $c = mp \geq 1 \cdot p = p > 1$ .