Assignment 4

Weishi Wang, ID 260540022

February 15, 2018

Problem 1. ***Division algorithm***

The division algorithm states that for any a,b $\in \mathbb{Z}$ ($b \neq 0$) there exist q,r $\in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$; furthermore, these q, r are unique for a, b. We proved this when a, $b > 0$. Prove that q, r exist for all a, b. Hints: (1) You may use the fact that the statement holds when a, $b > 0$ as a tool without proving it and (2) you will need to consider cases.

Solution. We have proven the case a,b>0.

Let's consider other cases.

Case 1: a>0 and b<0:

Look at the following multiple of b:

0, -b, -2b, -3b,...

There is some multiple of b that is greater than a. [ex: -(2a)b = (-2b)a $\geq$ a]

Let B = { kb | k$\in \mathbb{Z}$, kb > a}

By the well ordering principle, B. has a smallest element, call it q-1. (q<0)

Then, since (q-1)b is the smallest element that is greater than a, qb must be smaller or equal to a:

qb $\leq$ a < (q-1)b

let r = a - qb

Then,

0 $\leq$ r < (q-1)b - 1b

0 $\leq$ r < -b

Since b < 0, we have:

0 $\leq$ r < $|b|$

Case 2: a=0 and b>0:

if a=0, then r = -qb

let q = 0, then r = 0

Then 0 $\leq$ r < b is satisfied.

Case 3: a=0 and b<0:

Same proof as in Case 2.

Case 4: a<0 and b>0:
Let B = $\{$kb $|$ k $\in \mathbb{Z}$, kb < -a$\}$
The well ordering principle says that there exists a least integer greater than some number.
Therefore, in this set, it must exist a largest integer smaller than -a (which is positive).
Find the greatest element in B and call it (-q-1)b. (q>0)
Since (-q-1)b is the greatest element smaller than -a, (-q-1)b+b must be greater or equal to -a:
(-q-1)b < -a $\leq$ (-q-1+1)b
(-q-1)b < -a $\leq$ -qb
Since a = qb +r, then -a = -qb -r.
(-q-1)b < -qb-r $\leq$ -qb
(-q-1)b + qb < -r $\leq$ -qb + qb
-b < -r $\leq$ 0
0 $\leq$ r < b
Since b > 0, b = $|b|$
0 $\leq$ r < $|b|$

Case 5: a<0 and b<0:
Let B = $\{$kb $|$ k $\in \mathbb{Z}$, kb < -a$\}$
Find the greatest element in B and call it (-q+1)b. (q>0 and b<0)
Since (-q+1)b is the greatest element smaller than -a, (-q+1)b-b must be greater or equal to -a (Since b<0):
(-q+1)b < -a $\leq$ -qb
(-q+1)b < -a $\leq$ -qb
Since a = qb +r, then -a = -qb -r.
(-q+1)b < -qb-r $\leq$ -qb
(-q+1)b + qb < -r $\leq$ -qb + qb
b < -r $\leq$ 0
0 $\leq$ r < -b
Since b < 0, -b = $|b|$
0 $\leq$ r < $|b|$

Moreover, b cannot be 0, therefore all cases are considered.

Problem 2. *Divisors*

(a) Find gcd(2018, 240), and express you answer as a linear combination of 2018 and 240 (that is, find r, s $\in \mathbb{Z}$ such that gcd(2018, 240) = 2018r + 240s).

(b) Let k be a positive integer. Show that if a and b are relatively prime integers, then gcd(a+kb,b+ka) divides k^2-1. Hint: Consider two linear combinations of a + kb and b + ka.

(c) Suppose n, m, $p \in \mathbb{N}$, p a prime, where $p \mid n$, $m \mid n$, and $p \nmid m$. Either prove that p divides $\frac{n}{m}$ or provide a counterexample to show that it doesn't. Make sure to address whether or not "p divides $\frac{n}{m}$" even makes sense.

Solution. (a) Apply Euclidean Algorithm:
2018 = 8 × (240) + 98
240 = 2 × 98 + 44
98 = 2 × 44 + 10
44 = 4 ×10 + 4
10 = 2 × 4 + 2
4 = 2 × 2 + 0
Thus, gcd(2018, 240) = 2

2 = 10 - 2 × 4
= 10 - 2[44 - 4(10)]
= 9(10) - 2(44)
= 9(98-2(44)) - 2(44)
= 9(98) - 20(44)
= 9(98) - 20(240 - 2(98))
= 49(98) - 20(240)
= 49(2018 - 8(240)) - 20(240)
= 49 × 2018 - 412 × 240

Thus,
2 = (49 × 2018) - (412 × 240)

(b) Consider the lemma: if g | a and g | b, then g | xa + yb, ∀ x,y $\in\mathbb{Z}$
Proof: g | a, then pg = a, p $\in\mathbb{Z}$
g | b, then qg = b, q$\in\mathbb{Z}$
xa + yb = xpg + yqg, x,y,p,q$\in\mathbb{Z}$
xa + yb = (px + qy)g, x,y,p,q$\in\mathbb{Z}$
so g | (xa+yb).
Which means that g divides any linear combination of a and b.

Now consider the question:
Let g = gcd(a+kb, b+ka)
consider the linear combination -(a+kb)+k(b+ak).
By lemma, we know that g | [-(a+kb)+k(b+ak)].
⇒ g | [a($k^2 - 1$)].

consider another linear combination k(a+kb)-(b+ak).
By lemma, we know that g | [k(a+kb)-(b+ak)].
⇒ g | [b($k^2 - 1$)].

Thus, g | [a(k^2-1)] and g | [b(k^2-1)].

There are 4 possibilities:
(1) g | (k^2-1) and g | a
(2) g | (k^2-1) and g | b
(3) g | (k^2-1)
(4) g | b and g | a

However, (4) is not possible since a and b are relatively prime, g cannot divide both of them.
Only (1), (2) and (3) are possible.
They all imply that g | (k^2-1).
Therefore, gcd(a+kb,b+ka) divides k^2-1.

(c) We divide by p and m, so p,m≠0.
if n=0, then any number divides n. so p | $\frac{n}{m} \Rightarrow$ p | 0, which is always true.

The problem states that n,p,m $\in \mathbb{N}$, which does not include 0. So we don't really need to consider cases, but it does not affect the solution.

if n≠ 0:
p∤m and p is prime means that gcd(p,m) = 1.
So there are no components in p and m can be canceled.
p | n, m | n, and gcd(p,m)=1 means that n must be composed of at least one p and one m.
This implies that pm|n.
k(pm) = n, k∈$\mathbb{Z}$
kp = $\frac{n}{m}$, k∈$\mathbb{Z}$
$\Rightarrow$ p | $\frac{n}{m}$.

In addition, p divides $\frac{n}{m}$ makes sense when $\frac{n}{m}$ is an integer. The problem states that m | n, therefore $\frac{n}{m}$ must be integer when m ≠ 0.

Problem 3. ***Congruence and modular arithmetic***
(a) Let $k \in \mathbb{Z} \setminus \{0\}$. Prove that ka ≡ kb (mod kn) if and only if a ≡ b (mod n).

(b) Prove that if a ≡ b (mod n), then gcd(a,n) = gcd(b,n).

(c) Show that $1806^{6236} \equiv 1$ (mod 17).

Solution. (a) ka ≡ kb (mod kn)
$\Leftrightarrow$ kn|(ka -kb)

$\Leftrightarrow$ (ka - kb) = xkn, x $\in \mathbb{Z}$
$\Leftrightarrow$ (a-b) = xn, x $\in \mathbb{Z}$ (Since k $\neq$ 0)
$\Leftrightarrow$ n|(a-b)
$\Leftrightarrow$ a $\equiv$ b (mod n)

(b) a $\equiv$ b (mod n)
$\Rightarrow$ n|(a-b) $\Rightarrow$ (a - b) = kn, k $\in \mathbb{Z}$. (*)
Let g_1 = gcd(a,n) and g_2 = gcd(b,n)
Divide g_1 on both side of (*):
$\frac{a-b}{g_1} = \frac{kn}{g_1}$
$\frac{b}{g_1} = \frac{a}{g_1}$ - $\frac{kn}{g_1}$
since g_1 = gcd(a,n)
$\Rightarrow$ g_1|a and g_1|n
Thus, $\frac{a}{g_1}$, $\frac{kn}{g_1} \in \mathbb{Z}$
So, $\frac{b}{g_1} \in \mathbb{Z}$
$\Rightarrow$ g_1|b
This means that g_1|b and g_1|n
but g_2 is the gcd(b,n), so $g_1 \leq g_2$

Similarly, divide (*) by g_2, we obtain:
$\frac{a}{g_2} = \frac{b}{g_2} + \frac{kn}{g_2}$
g_2|b and g_1|n
So, g_2|a
This means that g_2|a and g_2|n
but g_1 is the gcd(a,n), so $g_2 \leq g_1$

Combine both result, we conclude that $g_1 = g_2$.

(c) 1086^{6236} (mod 17)
$\equiv (17\times106 + 4)^{6236}$ (mod 17)
$\equiv 4^{6236}$ (mod 17)
$\equiv (4^2)^{3118}$ (mod 17)
$\equiv 16^{3118}$ (mod 17)
$\equiv (17\text{-}1)^{3118}$ (mod 17)
$\equiv (\text{-}1)^{3118}$ (mod 17)
Since 3118 is an even number, $(\text{-}1)^{3118} = 1$.
Therefore $1086^{6236} \equiv 1$ (mod 17).