Assignment 4

Laetitia Fesselier, ID 260791354

February 14, 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.

Solution.

Case (1) a > 0, b > 0

There exits q, r $\in \mathbb{Z}$ such that a = qb + r and 0 $\leq$ r < | b |
See proof done in class.

q, r are unique for a, b $\in \mathbb{Z}$

See proof done in class.

Case (2) a = 0, b $\neq$ 0

For q = 0, r = 0, the statement is verified:
a = qb + r $\Rightarrow$ a = 0*b + 0 $\Rightarrow$ a = 0 and 0 $\leq$ r < | b |
So, the existence of such q, r is proven.

Case (3) a, b < 0

By case (1), we know that there exits q, r $\in \mathbb{Z}$ such that |a| = q|b| + r and 0 $\leq$ r < |b|

$$\begin{aligned} -\mid a \mid &= -q \mid b \mid -r && (*) \\ \Leftrightarrow -\mid a \mid &= -q \mid b \mid - \mid b \mid + \mid b \mid -r \\ \Leftrightarrow -\mid a \mid &= -(q+1) \mid b \mid + \mid b \mid -r && (**) \end{aligned}$$

Let be q'= -(q+1) and r' = | b | - r Replacing in (**), we have
-| a | = q'(-| b |) + r'
a = q'b + r'

(*) By case (1):
$0 \leq$ r < | b |
-| b | < -r $\leq$ 0
0 < |b| - r $\leq$ |b|
$0 \leq$ r'< | b | $\square$

<u>Case (4)</u> a < 0, b > 0

By case (1), we know that there exits q, r $\in \mathbb{Z}$ such that |a| = qb + r and $0 \leq$ r < |b|

$$\begin{aligned} & -\mid a \mid && = -qb - r && (*) \\ \Leftrightarrow & -\mid a \mid && = -qb - b + b - r && \\ \Leftrightarrow & -\mid a \mid && = -(q+1)b + b - r && (**) \end{aligned}$$

Let be q'= -(q+1) and r' = b - r Replacing in (**), we have
-| a | = q'b + r'
a = q'b + r'

(*) By case (1):
$0 \leq$ r < | b |
-| b | < -r $\leq$ 0
0 < |b| - r $\leq$ |b|
0 < b - r $\leq$ |b|
$0 \leq$ r'< | b | $\square$

<u>Case (5)</u> a > 0, b < 0

By case (3), we know that there exits q, r $\in \mathbb{Z}$ such that -|a| = -q|b| - r and $0 \leq$ r < |b|

$$\begin{aligned} & \mid a \mid && = q \mid b \mid + r \\ \Leftrightarrow & a && = qb + r \end{aligned}$$

$\square$

Problem 2. *Divisors*

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

Solution.

2018 = 8 × 240 + 98
240 = 2 × 98 + 44
98 = 2 × 44 + 10
44 = 4 × 10 + 4

$10 = 2 \times 4 + 2$
$4 = 2 \times 2 + 0$

$$\begin{aligned}
gcd(2018, 240) &= 2 \\
&= 10 - 2 \times 4 \\
&= 10 - 2 \times (44 - 4 \times 10) \\
&= 9 \times 10 - 2 \times 44 \\
&= 9 \times (98 - 2 \times 44) - 2 \times (240 - 2 \times 98) \\
&= 13 \times 98 - 18 \times 44 - 2 \times 240 \\
&= 13 \times (2018 - 8 \times 240) - 18 \times (240 - 2 \times 98) - 2 \times 240 \\
&= 13 \times 2018 - 104 \times 240 - 18 \times 240 + 36(2018 - 8 \times 240) - 2 \times 240 \\
&= 13 \times 2018 - 104 \times 240 - 18 \times 240 + 36 \times 2018 - 288 \times 240 - 2 \times 240 \\
&= 49 \times 2018 - 412 \times 240
\end{aligned}$$

(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.

Solution.

gcd(a, b) = 1 $\Leftrightarrow$ ma + nb = 1 (*)

Let consider the following linear combinations of a + kb and b + ka:
(k^2 - 1) nb = kn(a+kb) (1)
(k^2 - 1) ma = km(b+ka) (2)

Adding (1) and (2), we get:
(k^2 - 1) (ma + nb) = kn(a+kb) + km(b+ka)
$\Leftrightarrow$ (k^2 - 1) = kn(a+kb) + km(b+ka) using (*)

By definition, gcd(a + kb, b + ka) divides a + kb and b + ka.
Using the following LEMMA, if c | a and c | b, then c | xa + yb
for all x, y $\in \mathbb{Z}$, we can conclude that gcd(a + kb, b + ka) | k^2 - 1. $\square$

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

Solution.

We know m | n, so $\frac{n}{m} \in \mathbb{N}$. So p can possibly divides $\frac{n}{m}$.

Because p is prime, it can only be divisible by 1 or itself.
We also know that p $\nmid$ m, so the only common divisor of p and m is 1.
For this reason, gcd(p, m) = 1.

p | n $\Leftrightarrow$ p | m $\times$ $\frac{n}{m}$

Using the following corollary, If gcd(a,b) = 1 and a | bc, then a | c, with a = p, b = m, and c = $\frac{n}{m}$, we can conclude that p divides $\frac{n}{m}$.

Problem 3. *Congruence and modular arithmetic*

(a) Let k $\in \mathbb{Z}\backslash\{0\}$. Prove that ka $\equiv$ kb (mod kn) if and only if a $\equiv$ b (mod n)

Solution.

$$
\begin{aligned}
& ka \equiv \text{ kb (mod kn)} \\
\Leftrightarrow \quad & kn \mid (ka - kb) \\
\Leftrightarrow \quad & kn \mid k(a - b) \\
\Leftrightarrow \quad & n \mid (a - b) \\
\Leftrightarrow \quad & a \equiv \text{b (mod n)} \quad \square
\end{aligned}
$$

(b) Prove that if a $\equiv$ b (mod n), then gcd(a, n) = gcd(b, n).

Solution.

$$
\begin{aligned}
& a \equiv \text{b (mod n)} \\
\Rightarrow \quad & n \mid (a - b) \\
\Rightarrow \quad & a - b = qn \\
\Rightarrow \quad & a = qn + b \\
\Rightarrow \quad & gcd(a, n) = \text{gcd(b, n) (*)} \quad \square
\end{aligned}
$$

(*) Lemma : If a = qb + r, then gcd(a, b) = gcd(b, r) with b = n, r = b.

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

Solution.

(1) 1806 $\equiv$ 4 (mod 17)

(2) $4^4 \equiv 1$ (mod 17)

Using the following theorem:
if a $\equiv$ b (mod n) and x $\equiv$ y (mod n), ax $\equiv$ by (mod n)
We have:

$$
\begin{aligned}
1806 &\equiv 4 \text{ (mod 17)} \\
1806^{6236} &\equiv 4^{6236} \text{ (mod 17)} \\
1806^{6236} &\equiv (4^4)^{1559} \text{ (mod 17)} \\
1806^{6236} &\equiv 1^{1559} \text{ (mod 17)} \\
1806^{6236} &\equiv 1 \text{ (mod 17)} \qquad \square
\end{aligned}
$$