Homework 1 – MAS 2203 – Spring 2017

Section 1.2

#23

The conjecture is false.

We prove that if $p > 3$ is prime then either $3 \mid p+2$ or $3 \mid p+4$ so that either $p+2$ or $p+4$ is composite. Suppose $p > 3$ is prime. Then $3 \nmid p$ so by the division algorithm

$$p = 3q + r$$

for $q, r \in \mathbb{Z}$ with $r = 1$ or 2.

Case 1: $r = 1$. Then $p = 3q+1$, $p+2 = 3q+3 = 3(q+1)$ & $3 \mid p+2$.

Case 2: $r = 2$. Then $p = 3q+2$, $p+4 = 3q+6 = 3(q+2)$ & $3 \mid p+4$.

Hence either $3 \mid p+2$ or $3 \mid p+4$ & the Conjecture is false.

#24

Let $n \in \mathbb{Z}$ with $n > 11$.

Case 1: n is even. Then

$$n = 2q \quad \text{where } q \geq 6,\ q \in \mathbb{Z}.$$

$$n = 2(q-2) + 4.$$

$2(q-2)$ is composite since $q - 2 \geq 4$.

So n is the sum of two composites namely $2(q-2)$ & 4.

Case 2: n is odd. Then

$$n = 2q + 1 \quad \text{where } q \geq 6 \text{ \& } q \in \mathbb{Z}.$$

Then

$$n = 2(q-4) + 9.$$

$2(q-4)$ is composite since $q-4 \geq 2$.

So n is the sum of two composites namely

$2(q-4)$ & 9.

In both cases n is the sum of two composites

∎

#27

Let a, n be positive integers, $n \neq 1$.

Suppose $a^n - 1$ is prime.

Then $a > 1$ since $1^n - 1 = 0$ is not prime.

Also $n \geq 2$ since $n > 0$, $n \neq 1$ & $n \in \mathbb{Z}$.

Now,

$$a^n - 1 = (a-1)(1 + a + a^2 + \cdots + a^{n-1}).$$

So $a - 1 \mid a^n - 1$ since $(1 + a + \cdots + a^{n-1}) \in \mathbb{Z}$

Since $a > 1$, $a \geq 2$ &

$$1 \leq a - 1 < a^n - 1 \quad \text{since } a > 1 \text{ \& } n > 1.$$

Since $a^n - 1$ is prime this implies $a - 1 = 1$ &

$$a = 2.$$

We have $a^n - 1 = 2^n - 1$ is prime.

We prove in class that is implies n is prime.

<u>Section 1.3</u> Let $a, b \in \mathbb{Z}$ with a, b not both zero

#37 & let c be an nonzero integer.

We assume $c > 0$, so that $c = |c|$. The proof is similar when $c < 0$.

Let $S_1 = \{am + bn : m, n \in \mathbb{Z} \ \& \ am + bn > 0\}$,

$S_2 = \{acx + bcy : x, y \in \mathbb{Z} \ \& \ acx + bcy > 0\}$.

Then

$(a, b) = \min S_1$ & $(ac, bc) = \min S_2$

by Prop 1.11.

Let $d = (a, b)$. We claim that dc is smallest element of S_2. $d \in S_1$ so $d = am + bn$ where $m, n \in \mathbb{Z}$ & &

$dc = (ac)m + (bc)n \in S_2$.

Suppose by way of contradiction that $e \in S_2$ & $e < dc$.

Then $e = acx_1 + bcy_1$ for some $x_1, y_1 \in \mathbb{Z}$ &

$e = cf$ where $f = ax_1 + by_1 > 0$ &

So $f \in S_1$. Since $d = \min S_1$, $f \geq d$ &

$e = cf \geq cd$ which is a contradict to $e < dc$.

Hence $dc = \min(S_2)$ &

$dc = (ac, bc)$ by Prop. 1.11.

#38 Suppose a, b be relatively prime integers ie $(a,b) = 1$.

Let $\alpha = a + b$, $\beta = a - b$.

Then $\alpha + \beta = 2a$, $\alpha - \beta = 2b$.

Let $d = (a+b, a-b) = (\alpha, \beta)$. Then

$d | \alpha$ & $d | \beta$ so that $d | 2a$ & $d | 2b$.

From Prop 1.11, it follows that $d | (2a, 2b)$.

But $(2a, 2b) = 2(a, b) = 2$ by Ex 37. Hence $d = 1$ or 2.

#40 Let $a, b \in \mathbb{Z}$ with $(a,4) = (b,4) = 2$.
Hence $2 \mid a$ & $2 \mid b$ so a, b are even.
By the Division Alg.

$$a = 4q_1 + r_1 \quad \text{some } q_1, r \in \mathbb{Z}$$

$r = 0$ or 2. Since $(a,4) = 2$, $4 \nmid a$ &
$r = 2$. Similarly

$$b = 4q_2 + 2 \quad \text{some } q_2 \in \mathbb{Z}.$$

Hence

$$a + b = 4(q_1 + q_2) + 2 + 2 = 4(q_1 + q_2 + 1)$$

& $4 \mid a+b$. Hence

$$(a+b, 4) = 4.$$

#47
(a) Let $a, b \in \mathbb{Z}$ & m is a ~~nonnegative~~ positive integer.

($\Rightarrow$) Suppose $(a,b) = 1$.

~~$(a,b) = (a,b) = \dots\dots =$~~

$$\underbrace{(b, a) = (b, a) = \dots = (b, a)}_{(m\text{-}\mathrm{times})} = 1$$

By Ex 42(b), $(b, a^m) = (a^m, b) = 1$.

($\Leftarrow$) Suppose $(a^m, b) = 1$. Then by Prop. 1.11

$$a^m x + by = 1 \quad \text{some } x, y \in \mathbb{Z}, \&$$

$$a(a^{m-1}x) + by = 1 \quad \&$$

$(a, b) = 1$ again by Prop. 1.11.

(b) Let $a, b \in \mathbb{Z}$, m, n positive integers. By (a)

$$(a,b) = 1 \iff (a^m, b) = 1 \iff (a^m, b^n) = 1.$$

Section 1.4

(*) Let $a = 4331$, $b = 1342$.

$$4331 = 3 \cdot 1342 + 305 \qquad 305 = a - 3b$$

$$1342 = 4 \cdot 305 + 122 \qquad 122 = b - 4 \cdot 305$$

$$= b - 4(a - 3b)$$

$$= 13b - 4a$$

$$305 = 2 \cdot 122 + 61 \qquad 61 = 305 - 2 \cdot 122$$

$$122 = 2 \cdot 61 + 0 \qquad = (a - 3b) - 2(13b - 4a)$$

$$= 9a - 29b$$

By Euclidean Alg.

$$(a, b) = d = 61 \ \&$$

we see that

$$ax + by = d = 61 \quad \text{for } x = 9,\ y = -29.$$

(*) Let $a, b, c, d \in \mathbb{Z}$ where a, b are not both zero.
Let $d = (a, b)$.

($\Rightarrow$) Suppose $ax + by = c$ for some $x, y \in \mathbb{Z}$.
Since $d \mid a$ & $d \mid b$,

$$d \mid ax + by = c \ \& \ d \mid c$$

by Prop 1.2.

($\Leftarrow$) Suppose $d \mid c$. Then

$$c = de \quad \text{for some } e \in \mathbb{Z}.$$

Since $d = (a, b)$,

$$d = am + bn \quad \text{for some } m, n \in \mathbb{Z}$$

by Prop 1.11. Then

$$c = de = a(em) + b(en) = ax + by$$

where $x = em$ & $y = en \in \mathbb{Z}$.

Section 1.5

$a = 2^3 \cdot 3^2 \cdot 5^2 \cdot 13^7 \cdot 19^0$

$b = 2^5 \cdot 3^3 \cdot 5^0 \cdot 13^5 \cdot 19^1$.

(*) By Prop 1.17,

$$(a,b) = 2^3 \cdot 3^2 \cdot 5^0 \cdot 13^5 \cdot 19^0$$
$$= 2^3 \cdot 3^2 \cdot 13^5, \quad \&$$
$$[a,b] = 2^5 \cdot 3^3 \cdot 5^2 \cdot 13^7 \cdot 19^1$$

(*) # 70

(a) The statement is false.
For example let $a = 2^3 = 8$, $b = 2^2 = 4$.
Then $a^2 = 2^6 = b^3$ & $a^2 \mid b^3$
but $8 \nmid 4$ & $a \nmid b$.

(b) Suppose $a, b \in \mathbb{Z}$, $a, b > 0$ & $a^2 \mid b^2$.
Let $a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$,
$b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$
be prime factorizations of a, b where
$p_1, \ldots, p_r$ are distinct primes & each $e_j, f_j \geq 0$.
Then

$$a^2 = p_1^{2e_1} p_2^{2e_2} \cdots p_r^{2e_r}$$
$$b^2 = p_1^{2f_1} p_2^{2f_2} \cdots p_r^{2f_r}.$$

Since $a^2 \mid b^2$ each $2e_j \leq 2f_j$ by
a Prop. proved in class. Hence

$$e_j \leq f_j \text{ for each } j \ \&$$

$a \mid b$ by the same ~~Pro~~ Prop.