# MATH 4041 HW 7

David Chen, dc3451

October 25, 2020

I use that $a \mid b \implies |a| \leq |b|$ for nonzero $b$ a few times in this homework, and I can't recall if it was shown in class. I'll just show it here at the top of the problem set: $a \mid b \implies b = ak$ for some $k \in \mathbb{Z}$; then, since $b$ is nonzero, $k$ cannot be 0, so $k \neq 0$, then $k \geq 1$ or $k \leq -1$, so we have that $|ak| - |a| = (|k| - 1)|a|$, which is either 0 if $k = \pm 1$ or positive otherwise, so $|b| = |ak| \geq |a|$.

## Problem 1

1.

$$\begin{aligned} 11 &= 5 \cdot 2 + 1 \\ 1 &= 11 - 5 \cdot 2 \end{aligned}$$

so we can take $a^{-1} = -2, 9$, or more generally any $x \equiv -2 \equiv 9 \mod 11$.

2. $21^{-1} \mod 28$ does not exist, since $\gcd(21, 28) = 7$, and so there is no integer solution to $21x = 1 + 28y$.

3.

$$\begin{aligned} 101 &= 2 \cdot 50 + 1 \\ 1 &= 101 - 2 \cdot 50 \end{aligned}$$

so we can take $a^{-1} = -50, 51$, or more generally any $x \equiv -50 \equiv 51 \mod 101$.

4.

$$\begin{aligned} 101 &= 4 \cdot 25 + 1 \\ 1 &= 101 - 4 \cdot 25 \end{aligned}$$

so we can take $a^{-1} = -25, 75$, or more generally any $x \equiv -25 \equiv 76 \mod 101$.

## Problem 2

When $n = 2k$ is even, then $\gcd(2, n) \geq 2$ since $2 \mid 2$ and $2 \mid 2k$, so we have that $2x = 1 + ny$ has no integer solutions, and so no multiplicative inverse exists for 2 modulo $n$.

If $n = 2k + 1$ instead, note that $2k + 1 = n \implies 2k + 2 = n + 1 \implies 2(k + 1) \equiv 1 \mod n$, so $k + 1$ is a suitable inverse; in general, any $x \equiv k + 1 \mod n$ is a suitable inverse.

## Problem 3

We can show that the least positive integer $a$ such that when viewed as an element of $\mathbb{Z}/n\mathbb{Z}$, $\langle m \rangle = \langle a \rangle$ is $\gcd(n, m)$. In particular, we already have from class that $\langle m \rangle = \langle \gcd(n, m) \rangle$; note that if $\gcd(n, m) = 1$, we are done as 1 is the least positive integer. If there is some $1 \leq a < \gcd(n, m)$ such that $\langle \gcd(n, m) \rangle = \langle a \rangle$, then we have that $a \in \langle \gcd(n, m) \rangle \implies a \equiv \gcd(n, m)x \mod n$ for some $x$, so $a = \gcd(n, m)x + ny$ for some $x, y \in \mathbb{Z}$; however, since $a < \gcd(n, m) \implies \gcd(\gcd(n, m), n) = \gcd(n, m) \nmid a$, this has no solutions, so $\Rightarrow\Leftarrow$ and $\gcd(n, m)$ is the least positive integer that generates $\langle m \rangle$ as an element of $\mathbb{Z}/n\mathbb{Z}$.

### i

The order is 12, as we saw in class that the order is $36/\gcd(21, 36)$, and similarly we have $a = \gcd(21, 36) = 3$.

### ii

The order is 3, as we saw in class that the order is $45/\gcd(30, 45)$, and similarly we have $a = \gcd(30, 45) = 15$.

### iii

By earlier homeworks, the order is $\operatorname{lcm}(12, 3) = 12$.

## Problem 4

For $0 \leq a < 11$, $[a]_{11} \in (\mathbb{Z}/11\mathbb{Z})^*$ only if $\gcd(a, 11) = 1$. Since 11 is prime, this is everything $1 \leq a \leq 10$, so the order is 10, as $[1]_{11}, [2]_{11}, \ldots, [10]_{11} \in (\mathbb{Z}/11\mathbb{Z})^*$.

We can find an explicit generator, so $(\mathbb{Z}/11\mathbb{Z})^*$ is cyclic and thus isomorphic to $\mathbb{Z}/10\mathbb{Z}$ (brackets dropped in the table):

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $2^n$ | 1 | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |

The order of any subgroup of $(\mathbb{Z}/11\mathbb{Z})^* \cong \mathbb{Z}/10\mathbb{Z}$ has order dividing 10, and this subgroup is the unique subgroup with that order.

Then, we have that the subgroups of $(\mathbb{Z}/11\mathbb{Z})^*$ are $\langle 1\rangle, \langle 2\rangle, \langle 4\rangle$, and $\langle 10\rangle$, which have orders $1, 10, 5, 2$ respectively, as can be checked in the table; this is given since the subgroup of order $d$ is generated by $2^{n/d}$, as seen in class for any divisor $d$ of 10.

# Problem 5

From class, every subgroup can be given by the form $\langle d\rangle$ for some divisor $d$ of $n$, as for any $a$, $\langle a\rangle = \langle \gcd(a, n)\rangle$. Then, since there is at most one subgroup of any given order in $\mathbb{Z}/n\mathbb{Z}$, the subgroups are (generators are computed by taking all $1 \leq g \leq 18$ with the same order $\gcd(g, n)$):

1. $\mathbb{Z}/18\mathbb{Z} = \langle 1\rangle = \langle 5\rangle = \langle 7\rangle = \langle 11\rangle = \langle 13\rangle = \langle 17\rangle$ which has order 18. Also, $\varphi(18) = 6$
2. $\langle 2\rangle = \langle 4\rangle = \langle 8\rangle = \langle 10\rangle = \langle 14\rangle = \langle 16\rangle$ which has order 9. Also, $\varphi(9) = 6$.
3. $\langle 3\rangle = \langle 15\rangle$ which has order 6. Also, $\varphi(6) = 2$.
4. $\langle 6\rangle = \langle 12\rangle$ which has order 3. Also, $\varphi(3) = 2$.
5. $\langle 9\rangle$ which has order 2. Also, $\varphi(2) = 1$.
6. $\langle 18\rangle = \langle 0\rangle$ which has order 1. Also, $\varphi(1) = 1$.

the totient of $n$ is calculated by counting the amount of generators of order $n$, which is an equivalence shown in class. Adding, we have that $\sum_{d|18} \varphi(d) = 1 + 1 + 2 + 2 + 6 + 6 = 18$.

# Problem 6

## a

$(\implies)$ We have that $d \mid a \implies a = dk$ for some $k \in \mathbb{Z}$. Then, $[d]_n^k = k \cdot [d]_n = [kd]_n = [a]_n \implies [a]_n \in \langle [d]_n\rangle$, which was what we wanted.

$(\impliedby)$ We have that $[a]_n \in \langle [d]_n\rangle \implies [a]_n = t \cdot [d]_n$ for $t \in \mathbb{Z} \implies [a]_n = [td]_n$. Then, by the construction of these equivalence classes, $a = td + nu$ for $u \in \mathbb{Z}$. However, we have that $d \mid n \implies n = dv$ for $v \in \mathbb{Z}$. Finally, we arrive at $a = td + uvd = d(t + uv)$, so $d \mid a$.

### b

( $\implies$ ) $a \equiv a' \mod n \implies a = a' + nt$ for some $t \in \mathbb{Z} \implies a = a' + tud$ as $d \mid n \implies n = du$ for some $u \in \mathbb{Z}$; then, $d \mid a \implies a = vd$ for $v \in \mathbb{Z}$, so $a' = vd - tud = d(v - tu)$ so $d \mid a'$.

( $\impliedby$ ) The above proof is symmetric; replace $a$ with $a'$ and vice versa.

$a' \equiv a \mod n \implies a' = a + nt$ for some $t \in \mathbb{Z} \implies a' = a + tud$ as $d \mid n \implies n = du$ for some $u \in \mathbb{Z}$; then, $d \mid a' \implies a' = vd$ for $v \in \mathbb{Z}$, so $a = vd - tud = d(v - tu)$ so $d \mid a$.

### c

Let $a' = a + nk$ for $k \in \mathbb{Z}$. Then, if $d \mid a$ and $d \mid n$, we have that $d \mid a + nk = a'$; similarly, if $d \mid a'$ and $d \mid n$, $d \mid a' - nk = a$, so we have that for any integer $d$, that $d \mid a$ and $d \mid n \implies d \mid a'$, as well as $d \min a'$ and $d \mid n \implies d \mid a$. Then take $d = \gcd(a, n)$ so by definition of the gcd, we have that $\gcd(a, n) \mid a$, $\gcd(a, n) \mid n$, so $\gcd(a, n) \mid a'$. However, this then gives that $\gcd(a, n) \mid \gcd(a', n)$, and since they are both positive, $\gcd(a, n) \leq \gcd(a', n)$. Taking $d = \gcd(a', n)$, we see that $\gcd(a', n) \mid a$ as well, so $\gcd(a', n) \mid \gcd(a, n)$, and $\gcd(a', n) \leq \gcd(a, n)$, so combining with before, $\gcd(a, n) = \gcd(a', n)$.

# Problem 7

Note that the existence of integers $x, y$ such that $1 = ax + by$ gives that $gcd(a, b) \mid 1$, but the only positive divisor of 1 is 1, so $\gcd(a, b) = 1$.

### i

Since $a, b$ are relatively prime, $1 = ax + by$ for some $x, y$; then, for any divisor $d$ of $a$, $a = dk$ for some $k \in \mathbb{Z}$, so $1 = dkx + by$, so there are integers $kx, y$ satisfying $1 = d(kx) + by$, so from class $\gcd(d, b) = 1$.

### ii

Since $a$ is relatively prime to $n, m$, we can write $1 = ax + ny = aw + mz$; then, we have that $1 = (ax + ny)(aw + mz) = a^2xw + awny + axmz + nmyz = a(axw + wny + xmz) + nm(yz)$, so by class, $1 = \gcd(a, nm)$.

If $a$ is relatively prime to $mn$, then $1 = ax + nmy$, so there are integers $x, my$ such that $1 = ax + n(my)$, so $\gcd(a, n) = 1$; similarly, there are integers $x, ny$ such that $1 = ax + m(xy)$, so $\gcd(a, m) = 1$.

# Problem 8

## i

We can define $\text{lcm}(a, b)$ to be a positive integer $m$ such that $a \mid m$ and $b \mid m$; further, if $a \mid n$ and $b \mid n$ for some integer $n$, then $m \mid n$ as well.

To see that this is unique, suppose that $m, m'$ have the above property. Then, $m \mid m' \implies |m| \leq |m'|$ and $m' \mid m \implies |m'| \leq |m|$ Since both $|m| \leq |m'|$ and $|m'| \leq |m|$, and both are positive, $m = m'$.

## ii

We have that any element $mk \in \langle m \rangle$ satisfies that $mk \in \langle a \rangle \implies mk = ak'$ and $n \in \langle b \rangle \implies mk = bk''$ for $k', k'' \in \mathbb{Z}$, so all elements of $\langle m \rangle$ are common multiples of $a, b$. In particular, if $k = 1$, then $m = ak' = bk''$, so $a \mid m$ and $b \mid m$. Further, any common multiple of $a, b$ is an element of $\langle a \rangle \cap \langle b \rangle$: a common multiple is some number $l$ such that $l = ak' = bk''$, but this is exactly the condition to be in $\langle a \rangle \cap \langle b \rangle$, since $l = ak' \implies l \in \langle a \rangle$, and $l = bk'' \implies l \in \langle b \rangle$. Further, there is no element $n$ in $\langle m \rangle$ such that $1 \leq n < m$ as then $m \nmid n$ (since $m \mid n \implies m \geq n$), so $m$ is the least positive integer in the list of common multiples of $a, b$, which we just saw to be $\langle a \rangle \cap \langle b \rangle$, and in that sense is the least common multiple.

Then, clearly $m \mid mk$ for $k \in \mathbb{Z}$, so this also satisfies the definition of part i, as $m \mid mk = ak' = bk''$ (since for any $n$, $a \mid n, b \mid n \implies n = ak', n = bk'', k', k'' \in \mathbb{Z} \implies n = mk$ for some integer $k$, as shown earlier).

## iii

If $a \mid bk$ for some $k \in \mathbb{Z}$, then $a \mid k$ by a lemma from class since $a, b$ are relatively prime. Now, for any common multiple $n$, if $a \mid n$ and $b \mid n$, we have that $n = bk$ for some $k$, so $n = b(ak') = (ab)k'$ for some $k' \in \mathbb{Z}$ since $a \mid n = bk$ and thus $a \mid k$. Then, $ab \mid n \implies |ab| \mid n$. Furthermore, clearly $a \mid |ab|$ and $b \mid |ab|$. This gives that $ab$ satisfies all the conditions in part i of the lcm.

## iv

Suppose that $e = \gcd\left(\frac{a}{d}, \frac{b}{d}\right) > 1$. Then, $e \mid a/d \implies e = (a/d)k \implies ed \mid a$; similarly, $e \mid b/d \implies ed \mid b$. However, we now have that $ed$ is a common factor of $a, b$, but since $e > 1 \implies ed > d$, $ed \nmid d$ (as $ed \mid d \implies ed \leq d$, since both are positive), so $d$ cannot be the gcd of $a, b$. $\Rightarrow\Leftarrow$, so $e = 1$, and $a, b$ are relatively prime.

## v

Put $e = \operatorname{lcm}\left(\frac{a}{k}, \frac{b}{k}\right)$. Then, $a/k \mid e \implies a/k = ek' \implies a = ekk' \implies a \mid ek$ and $b/k \mid e \implies b \mid ek$ similarly, so $ek$ is a common multiple.

Now let $n$ be any common multiple, so $a \mid n$ and $b \mid n$. Note that $a \mid n,\ k \mid a \implies k \mid n$. Let $n = kx, a = ky$, so $n/k = x$, $a/k = y$. Further, $a \mid n \implies n = ak', k' \in \mathbb{Z} \implies kx = kyk' \implies x = yk' \implies n/k = (a/k)k' \implies a/k \mid n/k$. Similarly, $b \mid n \implies b/k \mid n/k$, so $n/k$ is a common multiple of $a/k$ and $b/k$. Then, since $e = \operatorname{lcm}\left(\frac{a}{k}, \frac{b}{k}\right)$, we have that $e \mid n/k \implies e = (n/k)k', k' \in \mathbb{Z}, \implies ek = nk' \implies ek \mid n$, which was what we wanted.

## vi

From above, we have that $\operatorname{lcm}(a,b) = \gcd(a,b)\operatorname{lcm}\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right)$. From iv, we have that $\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}$ are relatively prime, and so from iii, $\operatorname{lcm}\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = \left|\frac{a}{\gcd(a,b)}\frac{b}{\gcd(a,b)}\right| = \frac{|ab|}{\gcd(a,b)^2}$. Then, finally, we get that $\operatorname{lcm}(a,b) = \gcd(a,b)\operatorname{lcm}\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = \frac{|ab|}{\gcd(a,b)}$.

## vii

If $a = \prod_{i=1}^{n} p_i^{r_i}, b = \prod_{i=1}^{m} q_i^{s_i}$. Consider $\{u \mid u = p_i, 1 \le i \le n, \text{ or } u = q_i, 1 \le i \le m\}$. Then, let

$$t_u = \begin{cases} \max(r_i, s_j) & u = p_i, u = q_j \\ r_i & u = p_i, u \neq q_j, 1 \le j \le m \\ s_i & u = q_i, u \neq p_j, 1 \le j \le n \end{cases}$$

We then have the following, if $\{u_i\}_{i=1}^{k}$ is some ordering of the earlier set:

$$\operatorname{lcm}(a,b) = \prod_{i=1}^{k} u_i^{t_{u_i}}$$

Morally, this is just saying that the lcm is the product of all the primes in factorizations of $a, b$ with the exponent chosen to be the greater of the two exponents in the factorizations of $a, b$ (if it only shows up in one factorization, pick the exponent in the one it shows up in).