

Fundamental Mathematics - 347 G1 Homework 6 – Solutions

1. **6.2.** The numbers relatively prime to p are any numbers which are not a multiple of p . To see this, notice that the only divisors of p are p and 1. Consider any $a \in \mathbb{Z}$: either $p \nmid a$ or $p|a$. If $p \nmid a$ then $\gcd(a, p) = 1$, and if $p|a$ then a is a multiple of p .
2. **6.6.** It takes two steps if $n > 1$. (If $n = 0$ it takes no steps, and if $n = 1$ then it takes one step.) The remainder of $n + 1$ when dividing by n is always 1, so after one step we are left with $(1, n)$. Since $1|n$, the next step gives $(1, 0)$.
3. **6.11.** If we have k of each coin, then we have $91k$ cents. For this to be equal to a whole number of dollars, there needs to be some $n \in \mathbb{Z}$ with

$$91k = 100n.$$

What is the smallest (positive) value of k which does this? The right-hand side is clearly divisible by 100, and then so is the left-hand side. This gives

$$100|91k.$$

By Proposition 6.6 in the book, since $\gcd(100, 91) = 1$, this means that $100|k$. The smallest positive k for which this is true is $k = 100$. So we have 100 of each coin, which gives us \$91.

Without pennies, the equation becomes

$$90k = 100n.$$

Now, since $\gcd(90, 100) \neq 1$, we cannot use the same argument directly. But we can divide both sides of the equation by 10 to obtain

$$9k = 10n.$$

Since $\gcd(9, 10) = 1$, this means $10|k$, so we pick $k = 10$.

Without pennies or nickels, we get

$$85k = 100n,$$

dividing by 5 gives

$$17k = 20n,$$

so that $20|k$ and we choose $k = 20$.

4. **6.16.** We show the proof assuming $a, b \geq 0$. The same idea works if $a < 0 \vee b < 0$ but the proof is a bit more technical.

We first need to decide how we are going to choose k . Define the set S by

$$S = \{n \in \mathbb{N} : nb > a\}.$$

This set is nonempty and thus has a least element, which we call l . We then define $k = l - 1$. There are two facts we need about k :

- $kb \leq a$: if $kb > a$, then k would be in S , and since $k < l$, this means l would not be the least element in S .
- $(k + 1)b > a$: This is because $k + 1 = l$ and by definition $l \in S$.

Now, we claim that $r = a - kb$ must satisfy $0 \leq r \leq b - 1$. If $kb \leq a$, then $a - kb \geq 0$. So $r \geq 0$. Now use the fact that $(k + 1)b > a$, or $a - kb < b$. Since $a - kb \in \mathbb{Z}$, this means $a - kb \leq b - 1$.

So we have demonstrated at least one way to choose k, r . We now want to show that this choice is unique, up to the specification that $0 \leq r \leq b - 1$. So assume that we have two solutions: i.e.

$$a = kb + r, \quad a = k'b + r'.$$

Subtracting these from each other gives

$$b(k - k') + r - r' = 0,$$

or

$$(r - r')|b.$$

Since we are restricting $0 \leq r, r' \leq b - 1$, this means that

$$-(b - 1) \leq r - r' \leq b - 1.$$

This combined with $(r - r')|b$ gives $r - r' = 0$ or $r = r'$.

5. **6.18.** To answer the first question, yes: if $\gcd(a, b) = 1$ then $\gcd(a^2, b^2) = 1$ as well. We show two proofs of this.

(a) Let us consider at the prime factorization. We write

$$\begin{aligned} a &= p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}, \\ b &= p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}. \end{aligned}$$

If $\gcd(a, b) = 1$, this means that $\min(a_k, b_k) = 0$ for all k . (If not, i.e. if $a_k > 0$ and $b_k > 0$ for some k , then both a and b are divisible by p_k .) But then notice that

$$\begin{aligned} a^2 &= p_1^{2a_1} p_2^{2a_2} \dots p_k^{2a_k}, \\ b^2 &= p_1^{2b_1} p_2^{2b_2} \dots p_k^{2b_k}. \end{aligned}$$

Since $\min(a_k, b_k) = 0$ for all k , it follows that $\min(2a_k, 2b_k) = 0$ for all k , and so it follows that $\gcd(a^2, b^2) = 1$.

- (b) We prove this by contradiction. Let us assume that $\gcd(a, b) = 1$ and $\gcd(a^2, b^2) > 1$, i.e. there exists a $d > 1$ with $d|a^2 \wedge d|b^2$. Since $d > 1$, there is some prime p with $p|d$. Therefore there exists at least one prime with $p|a^2 \wedge p|b^2$. (Notice that $p > 1$ by definition, since it is prime.) By Prop. 6.7, if $p|a^2$ then it must be true that $p|a$. Similarly, if $p|b^2$, then $p|b$. Since $p|a \wedge p|b$, we have $\gcd(a, b) \geq p > 1$, and this is a contradiction.

As for the second question, the answer is no. For example, choose $a = 2$ and b odd. Then $\gcd(a, b) = 1$ but $\gcd(a, 2b) = 2$.

6. **6.22.** For which k does $k - 2|2k$? We break the proof into two cases: either k is even or k is odd.

- If k is odd, then so is $k - 2$, in which case $\gcd(k - 2, 2) = 1$, which implies $(k - 2)|k$. Stated another way, we must have

$$\frac{k}{k - 2} \in \mathbb{Z}.$$

Of course, $k/(k - 2) > 1$ for all $k \geq 2$. Therefore, if $(k - 2)|k$, then $k/(k - 2)$ must be at least two (since it must be an integer). So we want to find for which k we have

$$\frac{k}{k - 2} \geq 2,$$

which becomes $2k - 4 \leq k$ or $k \leq 4$. The only odd k which satisfy this are $k = 1, k = 3$, and we're only looking for $k \geq 3$, so the only possible odd solution is $k = 3$. Of course, $k = 3$ works, since $1|6$.

- If k is even, also $k - 2$ is even, so that both $k - 2$ and $2k$ are even, and share at least a common factor of 2. We write $k = 2l$, then we are trying to satisfy

$$(k - 2)|2k \text{ or } (2l - 2)|4l.$$

Notice that since we are only looking for $k \geq 3$ we can restrict attention to those l with $l \geq 2$. Factoring out the common factor of 2, this becomes

$$(l - 1)|2l.$$

Now, notice that $2l/(l - 1)$ is always greater than 2. If, moreover, it is less than 3, then it is not an integer. So we want to find all l such that

$$\frac{2l}{l - 1} \geq 3.$$

which is $3l - 3 \leq 2l$ or $l \leq 3$. Thus we have $l = 2, 3$ as possible solutions. Recall that $k = 2l$, so this gives possible solutions of $k = 4, 6$. To check that these work, we have $2|8$ and $4|12$, so they do.

Thus the solutions are $k = 3, 4, 6$.

7. **6.25.** The proof we show will use the notation of modular arithmetic; of course, we didn't introduce this notation until Chapter 7, and one can prove this question without that notation, but this proof is nicer.

Essentially, to prove this statement, we need to show that when we divide a_k by 3, the remainder is 0 when k is a multiple of 3 and not zero (1 or 2) when k is not a multiple of 3, i.e.

$$a_k \equiv 0 \pmod{3} \iff k \equiv 0 \pmod{3}.$$

In fact, we will show more. We show that if we list the remainders of this sequence when dividing by 3, we get the repeating sequence

$$110220110220110220\dots$$

Since every third number in this sequence is zero, and all the others are not, this implies that every third a_n is divisible by 3, and the others are not.

The next element of this sequence only depends on the previous two. Thus, if we ever have a case where two elements appear in a row which have appeared before, then the sequence repeats from that point. So, let us consider the following chart, where we are doing operations modulo 3:

x	y	$2x + y$
0	0	0
0	1	1
0	2	2
1	0	2
1	1	0
1	2	1
2	0	1
2	1	2
2	2	0

So, for example, if we ever see 11 in the sequence, we then follow this with 0. Similarly, if we have 10, we follow this with 2, etc. We know the sequence starts with 11, so we compute

$$11022011$$

Looking at the chart, we have 11 gives a 0, then 10 gives a 2, then 02 gives a 2, then 22 gives a 0, then 20 gives a 1, and 01 gives a 1. Now that we have 11 again, the sequence must repeat.

6.29. The best way to do this is with prime factorization. We write

$$\begin{aligned} a &= p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}, \\ b &= p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}. \end{aligned}$$

Define $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$. Then we expand

$$\begin{aligned} d &= p_1^{d_1} p_2^{d_2} \dots p_k^{d_k}, \\ m &= p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}. \end{aligned}$$

Now, what is the relationship amongst all of these exponents? We claim that

$$d_k = \min(a_k, b_k), \quad m_k = \max(a_k, b_k).$$

Let us first prove this for d_k . Notice that since $d|a$, we have $d_k \leq a_k$ for all k . Since $d|b$, we have $d_k \leq b_k$. Thus we have $d_k \leq \min(a_k, b_k)$. If $d_k < \min(a_k, b_k)$, then consider

$$\pi := p_k^{\min(a_k, b_k)}.$$

Clearly $\pi|a \wedge \pi|b$, and thus $\pi|\gcd(a, b)$. However, $\pi \nmid d$, since π has more powers of p_k in it than d does. This is a contradiction, so therefore it is not possible that $d_k < \min(a_k, b_k)$.

The proof that $m_k = \max(a_k, b_k)$ is quite similar.

So, now we have

$$\begin{aligned} ab &= p_1^{a_1+b_1} p_2^{a_2+b_2} \dots p_k^{a_k+b_k}, \\ \gcd(a, b) \cdot \text{lcm}(a, b) &= p_1^{d_1+m_1} p_2^{d_2+m_2} \dots p_k^{d_k+m_k}. \end{aligned}$$

If we can show that

$$a_k + b_k = d_k + m_k$$

for all k then we are done. However, this is the same as showing that

$$a_k + b_k = \min(a_k, b_k) + \max(a_k, b_k).$$

To see why this is true for any a_k, b_k , we reason as follows. One of the following three things are true: $a_k < b_k, a_k = b_k, a_k > b_k$. If $a_k < b_k$, then this equation becomes

$$a_k + b_k = a_k + b_k$$

which is true. If $a_k > b_k$, then the equation becomes

$$a_k + b_k = b_k + a_k,$$

which is also true. If $a_k = b_k$, then the equation becomes

$$2a_k = 2a_k,$$

again true. In all three cases, $a_k + b_k = \min(a_k, b_k) + \max(a_k, b_k)$ and thus $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$.

6.47. Take this equation and multiply it by 60, this gives

$$12x + 5y = 60. \tag{1}$$

Since $\gcd(12, 5) = 1$, this equation has integer solutions. Moreover, we know from discussion in lecture that to find all solutions to this equation, we need to only find one solution to (1), and all solutions to

$$12x + 5y = 0, \tag{2}$$

and the set of all solutions to (1) is that one particular solution we have found, plus the set of solutions to (2). We find a solution to (1) by inspection: observe that $(x = 5, y = 0)$ is one.

Now, to find all solutions to (2), or rewritten as

$$12x = -5y,$$

notice that since $\gcd(12, 5) = 1$, we must have that $12|y$ and $5|x$. Thus for some k , $x = 5k$, but then this implies $y = -12k$. So the set of all solutions to (2) can be written as

$$k(5, -12)$$

where $k \in \mathbb{Z}$. Thus all solutions to the original equation can be written as

$$x = 5 + 5k, \quad y = -12k, \quad k \in \mathbb{Z}.$$