MA 450 Homework 1

Josh Park

Fall 2024

Exercise 0.2

To find $\gcd(2^4 \cdot 3^2 \cdot 5 \cdot 7^2,\ 2 \cdot 3^3 \cdot 7 \cdot 11)$, we must find the common factors between the two values.
Both numbers share the factors 2, 3^2, 7.
Thus the GCD is $2 \cdot 3^2 \cdot 7 = 126$.

To find $\text{lcm}(2^3 \cdot 3^2 \cdot 5,\ 2 \cdot 3^3 \cdot 7 \cdot 11)$, we must find factors that are not common to both values.
These factors are 2^3, 3^3, 5, 7, 11.
Thus the LCM is $2^3 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 = 83160$.

Exercise 0.6

We wish to show for relatively prime integers a, b, that if $a \mid c$ and $b \mid c$, then $ab \mid c$.
We know that if a, b are relatively prime, then $\exists s, t \in \mathbb{Z}$ such that $as + bt = 1$.
Since $a \mid c$, it follows that $c = an$ for some $n \in \mathbb{Z}$. Similarly, $c = bm$ for some $m \in \mathbb{Z}$.

$$1 = as + bt \tag{1}$$
$$c = (as + bt)c = asc + btc \tag{2}$$
$$= asbm + btan = ab(sm + tn) \tag{3}$$

Thus c is divisible by ab.

Exercise 0.9

We are given that $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$.
By the division algorithm,

$$a \equiv a' \pmod{n} \implies xn + a' = a, \text{ for some } x \in \mathbb{Z} \tag{4}$$
$$b \equiv b' \pmod{n} \implies yn + b' = b, \text{ for some } y \in \mathbb{Z}. \tag{5}$$

We wish to show that $a + b \equiv a' + b'$ and $ab \equiv a'b' \pmod{n}$.
For the additive identity, notice that

$$a + b \equiv (xn + a') + (yn + b') \equiv (xn + yn + a' + b') \tag{6}$$
$$\equiv [(x + y)n + (a' + b')] \equiv a' + b' \pmod{n}. \tag{7}$$

Thus $(a + b) \bmod n = a' + b'$. For the multiplicative identity, note that

$$ab \equiv (xn + a')(yn + b') \tag{8}$$
$$\equiv xyn^2 + b'xn + a'yn + a'b' \equiv a'b' \pmod{n}. \tag{9}$$

Thus $(ab) \bmod n = a'b'$.

Exercise 0.12

We wish to show that $a = 5n + 3$ and $b = 7n + 4$ are relatively prime for all n.
We know a and b are relatively prime $\iff \exists s, t \in \mathbb{Z} \mid as + bt = 1$.
Thus, we only need to show that such integers s, t exist.
Consider the case when $s = 7$ and $t = -5$:

$$\begin{aligned} 7a + (-5)b &= 7(5n + 3) - 5(7n + 4) && (10)\\ &= 35n + 21 - 35n - 20 && (11)\\ &= 1 && (12) \end{aligned}$$

Thus $5n + 3$ and $7n + 4$ are relatively prime for all n.

Exercise 0.14

Taken mod 3, all integers fall into the equivalence classes [0], [1], or [-1].
We know a is a multiple of 3 $\forall a \in [0]$, so a is trivially a composite number (or 3 itself).
Thus for any prime number $p \neq 3$, it must be the case that either $p \in [1]$ or $p \in [-1]$.
That is, for any prime $p \neq 3$,

$$p \equiv 1 \pmod 3 \quad \text{or} \quad p \equiv -1 \pmod 3. \tag{13}$$

When we square p, notice that in both cases, $p^2 \equiv 1 \pmod 3$.
Thus for any primes p, q, r other than 3,

$$p^2 + q^2 + r^2 \equiv 1 + 1 + 1 \equiv 3 \equiv 0 \pmod 3. \tag{14}$$

Exercise 0.16

Notice that $7 \equiv 1 \pmod 3$.
By Exercise 0.9, if $a \equiv a' \pmod n$ and $b \equiv b' \pmod n$ then $ab \equiv a'b' \pmod n$.
Thus,

$$7^{1000} \equiv 1^{1000} \equiv 1 \pmod 6. \tag{15}$$

Similarly, $6 \equiv -1 \pmod 7$, whence

$$6^{1001} \equiv (-1)^{1001} \equiv -1 \pmod 7. \tag{16}$$

Exercise 0.27

Let $H \subseteq S$, where S contains n elements.
Our base case is when $n = 1$.
When S only has one element, there can trivially only be 2 possible subsets: S, and the empty set.
Thus $2^1 = 2$ proves our base case.
Assume this holds for n.
For $n + 1$, notice that we are able to create all previous subsets as they were, along with a new "copy" of each subset that now includes the new element.
Thus, the number of subsets is twice as much as the previous iteration.
Thus $2^n \cdot 2 = 2^{n+1}$, so our statement holds for $n + 1$.

Exercise 0.28

Our base case is when $n = 1$, and

$$2^n 3^{2n} - 1 = 2 \cdot 3^2 - 1 = 18 - 1 = 17. \tag{17}$$

Suppose this holds for n. We wish to show that this also holds for $n + 1$.

$$2^{n+1}3^{2(n+1)} - 1 = 2^{n+1}3^{2n+2} - 1 \tag{18}$$

$$= 2^n 3^{2n}[(2 \cdot 3^2 - 1) + 1] - 1 \tag{19}$$

$$= 2^n 3^{2n}(2 \cdot 3^2 - 1) + 2^n 3^{2n} - 1 \tag{20}$$

By the inductive hypothesis and base case respectively, $2^n 3^{2n} - 1$ and $2 \cdot 3^2 - 1$ are divisible by 17.
It follows that any linear combination of the two is also a multiple of 17, whence the identity holds for $n + 1$.
Thus, $2^n 3^{2n} - 1$ is always divisible by 17.

Exercise 0.32

Proof by weak induction. By trying some combinations of 7 and 9, we find that we can make 7, 9, 14, 16, 18, 21, 23, 25, 27, 28, 30, 32, 34, 35, 36, 37, 39, 41, 42, 43, 44, 45, 46, 48, 49, 50, 51, 52, 53, 54...
I claim that 47 is the largest integer that can not be made with a positive linear combination of 7 and 9.
Let $S = \{7a + 9b \mid a, b \in \mathbb{Z}_{\geq 0}\}$.
We wish to show that all integers ≥ 48 are in S.
Note that $3 \cdot 7 + 3 \cdot 9 = 48 \in S$.
Assume that some integer $n \in S$ such that $n \geq 48$, say $n = 7a + 9b$.
We must show that $n + 1 \in S$.
Notice that since $n \geq 48$, $a < 3$ and $b < 3$ cannot both be true.
If $a < 3$, then $n + 1 = (7a + 9b) + (4 \cdot 7 - 3 \cdot 9) = 7(a + 4) + 9(b - 3)$.
If $b < 3$, then $n + 1 = (7a + 9b) + (-5 \cdot 7 + 4 \cdot 9) = 7(a - 5) + 9(b + 4)$.
In the latter case it must be that $a \geq 5$, because $b = 2 \implies 9b = 18 \implies 7a \geq 30 \implies a \geq 5$.
Thus $n + 1 \in S$. □

Proof by strong induction. Let $S = \{7a + 9b \mid a, b \in \mathbb{Z}_{\geq 0}\}$.
I claim that 47 is the largest integer that is not in S.
Note that 48, 49, 50, 51, 52, 53, and 54 are all in S.
Assume that for some $n > 54$, S contains all integers k with $48 \leq k < n$.
We must show that $n \in S$.
Since $n - 7 \in S$, we know $\exists a, b \in \mathbb{Z}_{\geq 0}$ such that $n - 7 = 7a + 9b$.
But then $n = 7(a + 1) + 9b$. Thus $n \in S$. □