Math for CS 2015/2019 solutions to "In-Class Problems Week 5, Fri. (Session 12)"

https://github.com/spamegg1

October 25, 2022

Contents

1 Problem 1 **1**
1.1 (a) . . . 1
1.2 (b) . . . 2

2 Problem 2 **2**
2.1 (a) . . . 2
2.2 (b) . . . 2

3 Problem 3 **3**
3.1 (a) . . . 4
3.2 (b) . . . 5
3.3 (c) . . . 6

4 Problem 4 **6**
4.1 (a) . . . 6
4.2 (b) . . . 7
4.3 (c) . . . 7
4.4 (d) . . . 7

1 Problem 1

1.1 (a)

Use the Pulverizer to find integers x, y such that

$$30x + 22y = gcd(30, 22)$$

Proof. The GCD of $30 = 2 \cdot 3 \cdot 5$ and $22 = 2 \cdot 11$ is 2.

Here is the table produced by the Pulverizer:

x	y	$rem(x,y)$	$=$	$x = q \cdot y$
30	22	8	$=$	$30 - 1 \cdot 22$
22	8	6	$=$	$22 - 2 \cdot 8$
			$=$	$22 - 2 \cdot (30 - 1 \cdot 22)$
			$=$	$-2 \cdot 30 + 3 \cdot 22$
8	6	2	$=$	$8 - 1 \cdot 6$
			$=$	$(30 - 1 \cdot 22) - 1 \cdot (-2 \cdot 30 + 3 \cdot 22)$
			$=$	$\boxed{3 \cdot 30 - 4 \cdot 22}$
6	2	0		

Therefore $x = 3, y = -4$ and $30x + 22y = 30 \cdot 3 - 22 \cdot 4 = 90 - 88 = 2 = gcd(30, 22)$. □

1.2 (b)

Now find integers x', y' with $0 \leq y' < 30$ such that

$$30x' + 22y' = gcd(30, 22)$$

Proof. Since $(x, y) = (3, -4)$ works, so does $(3 - 22n, -4 + 30n)$ for any $n \in \mathbb{Z}$, so letting $n = 1$, we have $x' = -19, y' = 26$ and we have: $-19 \cdot 30 + 26 \cdot 22 = 2$. □

2 Problem 2

2.1 (a)

Let $m = 2^9 \cdot 5^{24} \cdot 11^7 \cdot 17^{12}$ and $n = 2^3 \cdot 7^{22} \cdot 11^{211} \cdot 13^1 \cdot 17^9 \cdot 19^2$. What is the $gcd(m, n)$? What is the least common multiple, $lcm(m, n)$ of m and n? Verify that

$$gcd(m, n) \cdot lcm(m, n) = m \cdot n \qquad (1)$$

Proof. $gcd(m, n) = 2^3 \cdot 11^7 \cdot 17^9$ and $lcm(m, n) = 2^9 \cdot 5^{24} \cdot 7^{22} \cdot 11^{211} \cdot 13^1 \cdot 17^{12} \cdot 19^2$.

Both $gcd(m, n) \cdot lcm(m, n)$ and $m \cdot n$ are equal to:

$$2^{9+3} \cdot 5^{24+0} \cdot 7^{0+22} \cdot 11^{7+211} \cdot 13^{0+1} \cdot 17^{12+9} \cdot 19^{0+2}$$

□

2.2 (b)

Describe in general how to find the $gcd(m, n)$ and $lcm(m, n)$ from the prime factorizations of m and n. Conclude that equation (1) holds for all positive integers m, n.

Proof. Assume that the prime factorizations of m and n are:

$$m = p_1^{m_1} \cdot \ldots \cdot p_a^{m_a} \text{ and } n = q_1^{n_1} \cdot \ldots \cdot q_b^{n_b}$$

(For example, say $m = 2^2 \cdot 5^3 \cdot 7^4$ and $n = 3^3 \cdot 5^2 \cdot 7^1 \cdot 11^2$. So $\{p_1, p_2, p_3\} = \{2, 5, 7\}$ and $\{q_1, q_2, q_3, q_4\} = \{3, 5, 7, 11\}$.)

Now the two sets of primes $p_1, \ldots, p_a$ and $q_1, \ldots . q_b$ might have some elements in common, and some different. Consider the union of these two sets of primes:

$$R ::= \{p_1, \ldots, p_a, q_1, \ldots . q_b\}$$

and let $\{r_1, \ldots, r_c\}$ be an enumeration of R, with all the possible repetitions removed.

(In our example, the primes 5 and 7 are common to both m and n.
So $\{r_1, r_2, r_3, r_4, r_5\} = \{2, 3, 5, 7, 11\}$.)

Now we can give an alternate way of writing the factorizations of m and n that includes all of the primes r_i, where, if a prime is missing in a factorization, we write it as having power 0:

$$m = r_1^{d_1} \cdot \ldots \cdot r_c^{d_c} \text{ and } n = r_1^{e_1} \cdot \ldots \cdot r_c^{e_c}$$

(In our example, this would give us: $m = 2^2 \cdot 3^0 \cdot 5^3 \cdot 7^4 \cdot 11^0$ and $n = 2^0 \cdot 3^3 \cdot 5^2 \cdot 7^1 \cdot 11^2$.)

This way, finding the GCD and the LCM is very simple: for each prime r_i, the GCD has the smaller of the two powers of r_i occurring in m and n, where the LCM has the larger of the two:

$$gcd(m, n) = r_1^{\min(d_1, e_1)} \cdot \ldots \cdot r_c^{\min(d_c, e_c)} \text{ and } lcm(m, n) = r_1^{\max(d_1, e_1)} \cdot \ldots \cdot r_c^{\max(d_c, e_c)}$$

Since for each i we have $\min(d_i, c_i) + \max(d_i, c_i) = d_i + c_i$, we have that both $gcd(m, n) \cdot lcm(m, n)$ and $m \cdot n$ are equal to

$$r_1^{d_1 + e_1} \cdot \ldots \cdot r_c^{d_c + e_c}$$

This proves $gcd(m, n) \cdot lcm(m, n) = m \cdot n$ for all positive integers m, n. □

3 Problem 3

The Binary GCD state machine computes the GCD of integers $a, b > 0$ using only division by 2 and subtraction, which makes it run very efficiently on hardware that uses binary representation of numbers. In practice, it runs more quickly than the more famous Euclidean algorithm described in Section 8.2.1 in the course textbook.

$$
\begin{array}{rcll}
\text{states} & ::= & \mathbb{N}^3 & \\
\text{start state} & ::= & (a, b, 1) & \\
\text{transitions} & ::= & \text{if } \min(x, y) > 0 \text{ then } (x, y, e) \to & \\
 & & (x/2, y/2, 2e) & \text{if } 2 \mid x \text{ and } 2 \mid y \\
 & & (x/2, y, e) & \text{else if } 2 \mid x \\
 & & (x, y/2, e) & \text{else if } 2 \mid y \\
 & & (x - y, y, e) & \text{else if } x > y \\
 & & (y - x, x, e) & \text{else if } y > x \\
 & & (1, 0, ex) & \text{otherwise } (x = y).
\end{array}
$$

3.1 (a)

Use the Invariant Principle to prove that if this machine stops, that is, reaches a state (x, y, e) in which no transition is possible, then $e = gcd(a, b)$.

Proof. First we have to find a preserved invariant of the machine. We have to guess what it is by working through a few examples.

I found this:

$$P((x, y, e)) ::= \ gcd(x, y) \cdot e = gcd(a, b)$$

Let's prove that this is a preserved invariant:

Start State. The start state is $(a, b, 1)$. We need to show $P((a, b, 1))$ is true. By definition:

$$P((a, b, 1)) ::= \ gcd(a, b) \cdot 1 = gcd(a, b)$$

which is clearly true.

Transitions. Assume $P((x, y, e))$ is true for some state (x, y, e). That is, $gcd(x, y) \cdot e = gcd(a, b)$.

Case: $2 \mid x$ **and** $2 \mid y$**.**

1. Assume $2 \mid x$ and $2 \mid y$. Then we need to show $P((x/2, y/2, 2e))$, in other words we need to show $gcd(x/2, y/2) \cdot 2e = gcd(a, b)$.

2. There exist integers m, n such that $x = 2m$ and $y = 2n$.

3. By our assumption $gcd(x, y) \cdot e = gcd(a, b)$, so $gcd(2m, 2n) \cdot e = gcd(a, b)$.

4. Notice that 2 is a common divisor of $2m$ and $2n$, so we have $gcd(2m, 2n) = 2 \cdot gcd(m, n) = 2 \cdot gcd(x/2, y/2)$.

5. By (3) and (4) we have

$$gcd(a, b) = gcd(2m, 2n) \cdot e = 2 \cdot gcd(m, n) \cdot e = gcd(m, n) \cdot (2e) = gcd(x/2, y/2) \cdot (2e)$$

which proves $P((x/2, y/2, 2e))$.

The next two cases are similar. Let's take a look at the fourth case:

Case: $2 \nmid x$ **and** $2 \nmid y$ **and** $x > y$**.** We need to show $P((x-y, y, e))$, in other words we need to show $gcd(x-y, y) \cdot e = gcd(a, b)$.

1. Assume $2 \nmid x$ and $2 \nmid y$ and $x > y$.

2. Assume c is an integer that divides both x and y. Then $c \mid (x-y)$ also.

3. Conversely, assume d is an integer that divides both $x-y$ and y. Then d also divides $x - y + y = x$.

4. By (2) and (3) the pair of integers $(x-y, y)$ and the pair of integers (x, y) have the same divisors.

5. Therefore $gcd(x-y, y) = gcd(x, y)$.

6. By our assumption $gcd(x, y) \cdot e = gcd(a, b)$.

7. By (5) and (6)

$$gcd(a, b) = gcd(x, y) \cdot e = gcd(x-y, y) \cdot e$$

which proves $P((x-y, y, e))$.

The fifth case is similar to the fourth. Finally the last case:

Case: $2 \nmid x$ **and** $2 \nmid y$ **and** $x = y$. We need to show $P((1, 0, ex))$, in other words we need to show $gcd(1, 0) \cdot ex = gcd(a, b)$.

1. By our assumption $gcd(x, y) \cdot e = gcd(a, b)$.

2. Since $x = y$, we have $gcd(x, y) = gcd(x, x) = x$.

3. By (1) and (2) $x \cdot e = gcd(a, b)$.

4. Notice that $gcd(1, 0) = 1$.

5. By (3) and (4) we have

$$gcd(a, b) = x \cdot e = ex = 1 \cdot ex = gcd(1, 0) \cdot ex$$

which proves $P((1, 0, ex))$.

This finishes the proof that P is a preserved invariant.

Since P is a preserved invariant, in a state (x, y, e) where no transition is possible, we must have $x = 1, y = 0$ and $P((1, 0, e))$ is true. So $gcd(1, 0) \cdot e = e = gcd(a, b)$ as desired. □

3.2 (b)

Prove that rule (2) $(x, y, e) \to (x/2, y/2, 2e)$ is never executed after any of the other rules is executed.

Proof. The rule $(x, y, e) \to (x/2, y/2, 2e)$ is executed only when both x and y are even. One of the other rules is executed if x and y are not both even (if at least one of them is odd).

So we need to show that, if the machine reaches a state (x, y, e) where at least one of x or y is odd, then we never reach a state again where x and y are both even.

So let's define this as a property, and prove that this property is a preserved invariant:

$P((x, y, e)) ::=$ If at least one of x or y is odd, then this is also true in the next state.

1. Assume at state (x, y, e) at least one of x and y is odd.

2. If x is even and y is odd, then the next state is $(x/2, y, e)$. In this next state, y is odd, so at least one of $x/2$ or y is odd, as needed.

3. If x is odd and y is even, then the next state is $(x, y/2, e)$. In this next state, x is odd, so at least one of x or $y/2$ is odd, as needed.

4. If x is odd and y is odd and $x > y$, then the next state is $(x - y, y, e)$. Then $x - y$ is even and y is odd, so at least one of them is odd, as needed.

5. If x is odd and y is odd and $y > x$, then the next state is $(y - x, x, e)$. Then $y - x$ is even and x is odd, so at least one of them is odd, as needed.

6. Finally if x is odd and y is odd and $x = y$ then the next state is $(1, 0, ex)$ where 1 is odd and 0 is even, so at least one of them is odd, as needed.

This proves P is a preserved invariant, proving (b). □

3.3 (c)

Prove that the machine reaches a final state in at most $1+3(\log(a)+\log(b))$ transitions. (This is a coarse bound; you may be able to get a better one.)

Proof. ??? □

4 Problem 4

For nonzero integers, a, b, prove the following properties of divisibility and GCD'S. (You may use the fact that $gcd(a, b)$ is an integer linear combination of a and b. You may not appeal to uniqueness of prime factorization because the properties below are needed to prove unique factorization.)

4.1 (a)

Every common divisor of a and b divides $gcd(a, b)$.

Proof. 1. By the fact above, there exist some integers s and t such that $gcd(a, b) = sa + tb$.

2. Assume c is a common divisor of a and b.

3. Since $c \mid a$, by definition of divisibility there exists an integer k such that $a = kc$.

4. Since $c \mid b$, by definition of divisibility there exists an integer m such that $b = mc$.

5. By (1), (4) and (5) we have $sa + tb = skc + tmc = c(sk + tm)$ so $c \mid sa + tb$, in other words $c \mid gcd(a, b)$. □

4.2 (b)

If $a \mid bc$ and $gcd(a, b) = 1$, then $a \mid c$.

Proof. 1. Since $gcd(a, b) = 1$, there exist integers s, t such that $sa + tb = 1$.

2. Multiplying (1) by c, we have $sac + tbc = c$.

3. Since $a \mid bc$, a divides the second term tbc of the sum in (2).

4. Obviously a also divides sac.

5. By (3) and (4) a divides $sac + tbc = c$. So $a \mid c$. □

4.3 (c)

If $p \mid bc$ for some prime p, then $p \mid b$ or $p \mid c$.

Proof. If p does not divide a, then since p is prime, $gcd(p, a) = 1$. By part (b), we conclude that $p \mid b$. □

4.4 (d)

Let m be the smallest integer linear combination of a and b that is positive. Show that $m = gcd(a, b)$.

Proof. To prove $m = gcd(a, b)$, we will prove $m \leq gcd(a, b)$ and $gcd(a, b) \leq m$.

Since $gcd(a, b)$ is positive and an integer linear combination of a and b, we have $m \leq gcd(a, b)$ (because m is the SMALLEST positive integer linear combination of a and b).

On the other hand, since m is a linear combination of a and b, every common divisor of a and b divides m.

So in particular, $gcd(a, b) \mid m$, which implies $gcd(a, b) \leq m$. □