Staff Solutions to In-Class Problems Week 5, Wed.

STAFF NOTE: Chapter 9. Number Theory through 9.4. Fundamental Theorem of Arithmetic

Problem 1.

(a) Use the Pulverizer to find integers $x, y$ such that

$$x30 + y22 = \gcd(30, 22).$$

Solution. Let $a = 30, b = 22$. Here is the table produced by the Pulverizer:

<table>
<thead>
<tr>
<th>$x$</th>
<th>$y$</th>
<th>$\text{rem}(x, y)$</th>
<th>$x - q \cdot y$</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>22</td>
<td>8</td>
<td>$a - b$</td>
</tr>
<tr>
<td>22</td>
<td>8</td>
<td>6</td>
<td>$b - 2 \cdot 8$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$= b - 2 \cdot (a - b)$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$= -2 \cdot a + 3 \cdot b$</td>
</tr>
<tr>
<td>8</td>
<td>6</td>
<td>2</td>
<td>$8 - 6$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$= (a - b) - (-2 \cdot a + 3 \cdot b)$</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>$= 3 \cdot a - 4 \cdot b$</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

so $(x, y) = (3, -4)$ works.

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

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

Solution. Since $(x, y) = (3, -4)$ works, so does $(3 - 22n, -4 + 30n)$ for any $n \in \mathbb{Z}$, so letting $n = 1$, we have

$$-19 \cdot 30 + 26 \cdot 22 = 2$$

Another possible answer is $(x', y') = (-8, 11)$, since in this case the gcd is 2.

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

$$\gcd(m, n) \cdot \text{lcm}(m, n) = mn.$$  \hspace{1cm} (1)
Solution.

\[ g = 2^311^717^9, \]
\[ l = 2^95^{24}7^{22}11^{211}13^117^{12}19^2 \]
\[ gl = 2^{12}5^{24}7^{22}11^{211}13^117^{21}19^2 = mn \]

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

Solution. Let \( v_k(n) \) be the largest power of \( k \) that divides \( n \), that is,

\[ v_k(n) := \max\{i \mid k^i \text{ divides } n\}. \]

Unique Prime Factorization now implies that for \( p \in \text{Primes}, \)

\[ v_p(mn) = v_p(m) + v_p(n), \quad (2) \]
\[ v_p(\gcd(m, n)) = \min\{v_p(m), v_p(n)\}, \quad (3) \]
\[ v_p(\text{lcm}(m, n)) = \max\{v_p(m), v_p(n)\}. \quad (4) \]

Therefore

\[ v_p(mn) = v_p(m) + v_p(n) \quad \text{(by (2))} \]
\[ = \min\{v_p(m), v_p(n)\} + \max\{v_p(m), v_p(n)\} \]
\[ = v_p(\gcd(m, n)) + v_p(\text{lcm}(m, n)) \quad \text{(by (3), (4))} \]
\[ = v_p(\gcd(m, n) \cdot \text{lcm}(m, n)) \quad \text{(by (2)).} \]

That is, \( mn \) and \( \gcd(m, n) \cdot \text{lcm}(m, n) \) have the same prime factorization, which proves (1).

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 9.2.1.

states ::= \( \mathbb{N}^3 \)
start ::= \((a, b, 1)\)
transitions ::= if \( \min(x, y) > 0 \), then \((x, y, e) \rightarrow \)
\[ (x/2, y/2, 2e) \quad \text{(if } 2 \mid x \text{ and } 2 \mid y) \quad (5) \]
\[ (x/2, y, e) \quad \text{(else if } 2 \mid x) \quad (6) \]
\[ (x, y/2, e) \quad \text{(else if } 2 \mid y) \quad (7) \]
\[ (x - y, y, e) \quad \text{(else if } x > y) \quad (8) \]
\[ (y - x, x, e) \quad \text{(else if } y > x) \quad (9) \]
\[ (1, 0, ex) \quad \text{(otherwise } x = y) \quad (10) \]
(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 \(e = \gcd(a, b)\).

**Solution.** We claim that a preserved invariant of this machine is

\[
\gcd(a, b) = e \gcd(x, y).
\]  

(11)

To show this, we assume the invariant holds for state \((x, y, e)\) and show that if \((x, y, e) \rightarrow (x', y', e')\), then \(\gcd(a, b) = e' \gcd(x', y')\).

The proof is by cases according to which kind of transition occurs.

**Case (5):** \((2 \mid x\) and \(2 \mid y\). In this case, \((x', y', e') = (x/2, y/2, 2e)\).

We use the easily verified fact

\[
\gcd(au, av) = a \gcd(u, v).
\]  

(12)

Now

\[
\gcd(a, b) = e \gcd(x, y) \quad \text{(by the invariant for \((x, y, e)\))}
= e2 \gcd(x/2, y/2) \quad \text{(by (12))}
= e' \gcd(x', y'),
\]

which shows that the invariant holds for \((x', y', e')\).

**Case (6):** \((2 \mid x\) and \(2 \nmid y\). In this case, \((x', y', e') = (x/2, y, e)\).

We use the easily verified fact

\[
\gcd(au, v) = \gcd(u, v)
\]  

(13)

for \(a\) relatively prime to \(v\).

Now

\[
\gcd(a, b) = e \gcd(x, y) \quad \text{(invariant for \((x, y, e)\))}
= e \gcd(x/2, y) \quad \text{(by (13))}
= e' \gcd(x', y'),
\]

which shows that the invariant holds for \((x', y', e')\).

**Case (8):** \((x > y, 2 \nmid x, \text{ and } 2 \nmid y)\)

In this case \((x', y', e') = (x - y, y, e)\).

We use the easily verified fact that

\[
\gcd(u - v, v) = \gcd(u, v).
\]  

(14)

Now,

\[
\gcd(a, b) = e \gcd(x, y) \quad \text{(invariant for \((x, y, e)\))}
= e \gcd(x - y, y) \quad \text{(by (14))}
= e' \gcd(x', y'),
\]

proving that the invariant holds for \((x', y', e')\).
Case (10): \((x = y)\). In this case, \((x', y', e') = (1, 0, ex)\). Now we have

\[
\gcd(a, b) = e \gcd(x, x) \quad \text{(by the invariant for \((x, x, e)\))}
\]
\[
= ex
\]
\[
= ex \gcd(1, 0) \quad \text{(since \(\gcd(1, 0) = 1\))}
\]
\[
= e' \gcd(x', y'),
\]

which shows that the invariant holds for \((x', y', e')\).

Verification of the remaining cases follows similarly.

To apply the Invariant Principle, we now first observe that the preserved invariant holds trivially in the start state \((a, b, 1)\) because \(\gcd(a, b) = 1 \cdot \gcd(a, b)\). We conclude that the preserved invariant holds in every reachable state.

We claim that only rule (10) can lead to a stopped state, which must be of the form \((1, 0, e')\). If such a state is reachable, then the invariant implies

\[
\gcd(a, b) = e' \gcd(1, 0) = e',
\]
as required.

To see why this is the only stopped state, note that a transition is always possible from the start state, and transitions (5)–(9) do not lead to stopped states since the minimum of the new \(x\) and \(y\) values remains positive.

(b) Prove that rule (5)

\[(x, y, e) \rightarrow (x/2, y/2, 2e)\]
is never executed after any of the other rules is executed.

**STAFF NOTE: Hint:** An invariant about the parity of \(x\) and \(y\).

**Solution.** We claim that another preserved invariant is

\[
\NOT(2 \mid x \ AND \ 2 \mid y)
\]

(15)

To verify this, suppose a state \((x, y, e)\) satisfies (15). Then rule (5) will not be executed in that state.

Suppose the second rule (6) gets executed leading to state \((x/2, y, e)\). Then \(x\) must be even and \(y\) must be odd, and so this state satisfies (15) since \(y\) is odd. A symmetric argument applies to the third rule (7).

If rule (8) gets executed leading to state \((x - y, y, e)\). Then if \(y\) is odd this state satisfies (15), and if \(y\) is even, then \(x\) must be odd, so this state satisfies (15) because \(x - y\) must be odd. A symmetric argument applies to rule (9).

Finally, rule (10) leading to state \((1, 0, ex)\) trivially satisfies (15) since 1 is odd.

Now if rule (5) is not executed in some state \((x, y, e)\), then (15) must hold, and since (15) is preserved, we can conclude that rule (5) will never be executed in any subsequent state.

(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.)

**Solution.** Either \(x\) or \(y\) gets halved after at most three transitions—the worst case is when \(x\) and \(y\) are both odd and \(y > x > 1\). In that case, the first transition switches \(x\) and \(y\), the next subtracts one from the other yielding an even value of \(x\), and the third transition will halve \(x\). So after at most \(3(\log a + \log b)\) transitions, one of \(x\) and \(y\) must have been reduced to 1, after which there can be at most one more transition.
Problem 4.
For nonzero integers, \( a, b \), prove the following properties of divisibility and GCD’S. (You may use the fact that \( \text{gcd}(a, b) \) 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.)

(a) Every common divisor of \( a \) and \( b \) divides \( \text{gcd}(a, b) \).

Solution. STAFF NOTE: Better proof is to use the fact that any common divisor, \( c \), of \( a \) and \( b \), is known to divide any linear combination of \( a \) and \( b \), and the gcd is such a linear combination.

For some \( s \) and \( t \), \( \text{gcd}(a, b) = sa + tb \). Let \( c \) be a common divisor of \( a \) and \( b \). Since \( c \mid a \) and \( c \mid b \), we have \( a = kc, b = k'c \) so

\[
sa + tb = skc + tk'c = c( sk + tk' )
\]

so \( c \mid sa + tb \).

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

Solution. Since \( \text{gcd}(a, b) = 1 \), we have \( sa + tb = 1 \) for some \( s, t \). Multiplying by \( c \), we have

\[
sac + tbc = c
\]

but \( a \) divides the second term of the sum since \( a \mid bc \), and it appears as a factor of the first term, and therefore it divides the sum, which equals \( c \).

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

Solution. If \( p \) does not divide \( b \), then since \( p \) is prime, \( \text{gcd}(p, b) = 1 \). By part (b), we conclude that \( p \mid c \).

(d) Let \( m \) be the smallest integer linear combination of \( a \) and \( b \) that is positive. Show that \( m = \text{gcd}(a, b) \).

Solution. Since \( \text{gcd}(a, b) \) is positive and an integer linear common of \( a \) and \( b \), we have

\[
m \leq \text{gcd}(a, b).
\]

STAFF NOTE: If there is time, challenge students to prove that \( m \) is a common divisor of \( a \) and \( b \) (and hence \( m \leq \text{gcd}(a, b) \)) without appealing to the fact that the gcd is a linear combination of \( a \) and \( b \):

It is enough to prove that \( m \mid a \). Suppose not. Then dividing \( a \) by \( m \) leaves a positive remainder. That is, \( a = qm + r \) for some \( r \in [1, m) \). But then \( r = a - qm \) is a smaller positive linear combination of \( a \) and \( b \), contradicting the definition of \( m \).

This now gives a proof that the gcd equals a linear combination, namely \( m \), that does not depend on the pulverizer.

On the other hand, since \( m \) is a linear combination of \( a \) and \( b \), every common factor of \( a \) and \( b \) divides \( m \). So in particular, \( \text{gcd}(a, b) \mid m \), which implies

\[
\text{gcd}(a, b) \leq m.
\]