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

STAFF NOTE: Number Theory: GCD’s, Ch. 8–8.4

Problem 1.

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

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

Solution. Here is the table produced by the Pulverizer:

<table>
<thead>
<tr>
<th>( x )</th>
<th>( y )</th>
<th>rem ((x, y))</th>
<th>( x - q \cdot y )</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>22</td>
<td>8</td>
<td>30 - 22</td>
</tr>
<tr>
<td>22</td>
<td>8</td>
<td>6</td>
<td>22 - 2 \cdot 8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>= 22 - 2 \cdot (30 - 22)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>= -2 \cdot 30 + 3 \cdot 22</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>= (30 - 22) - (-2 \cdot 30 + 3 \cdot 22)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>= 3 \cdot 30 - 4 \cdot 22</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>0</td>
<td>0</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 \( m = 2^95^2411^717^{12} \) and \( n = 2^37^{22}11^{211}13^117^919^2 \). What is the \( \gcd(m, n) \)? What is the least common multiple, \( \text{lcm}(m, n) \), of \( m \) and \( n \)? Verify that

\[ \gcd(m, n) \cdot \text{lcm}(m, n) = mn. \]

Solution.

\[ g = 2^311^717^9, \]
\[ l = 2^95^247^{22}11^{211}13^117^{12}19^2 \]
\[ gl = 2^{12}5^247^{22}11^{218}13^117^{21}19^2 = mn \]
(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 \(m, n\).

**Solution.** The divisors of \(m\) correspond to subsequences of the weakly increasing sequence of primes in the factorization of \(m\), and likewise for \(n\). So the factorization gcd \((m, n)\) is the largest common subsequence of the two factorizations. This can be calculated by taking all the primes that appear in both factorizations raised to the minimum of the powers of that prime in each factorization.

Likewise, the factorization of lcm \((m, n)\) is the shortest sequence that has the factorizations of \(m\) and \(n\) as subsequences. So the factorization of lcm \((m, n)\) can be calculated by taking all the primes that appear in either factorization raised to the maximum of the powers of that prime in each factorization.

So in the factorization of gcd \((m, n)\) · lcm \((m, n)\) each prime appears raised to a power equal to the sum of its powers in the factorizations of \(m\) and \(n\), which is precisely its power in the factorization of \(mn\).

**Problem 3.**

The binary-GCD state machine computes the GCD of \(a\) and \(b\) 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.

states ::= \(\mathbb{N}^3\)
start state ::= \((a, b, 1)\) (where \(a > b > 0\))
transitions ::= if \(\min(x, y) > 0\), then \((x, y, e) \rightarrow \) the first possible state according to the rules:

\[
\begin{cases}
(1, 0, ex) & \text{(if } x = y) \\
(1, 0, e) & \text{(if } y = 1), \\
(x/2, y/2, 2e) & \text{(if } 2 \mid x \text{ and } 2 \mid y), \\
(y, x, e) & \text{(if } y > x) \\
(x, y/2, e) & \text{(if } 2 \mid y) \\
(x/2, y, e) & \text{(if } 2 \mid x) \\
(x - y, y, e) & \text{(otherwise)}.
\end{cases}
\]

(a) 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.** Invariant is gcd \((a, b) = e \gcd(x, y)\). 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:** \((x = y)\). In this case we have \(\gcd(x, y) = x\) so by the invariant, gcd \((a, b) = ex\) gcd \((1, 0) = ex = \gcd(a, b)\), which shows that the invariant holds for \((x', y', e')\).

**Case:** \(2 \mid x \text{ and } 2 \mid y\). We use the fact that gcd \((ax, ay) = a \gcd(x, y)\).

(b) Prove that the machine reaches a final state in at most \(3 + 2 \log \max(a, b)\) transitions.

**Hint:** Strong induction on \(\max(a, b)\).
Solution.

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.)

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

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 $t$, $\gcd(a, b) = sa + tb$. 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 $\gcd(a, b) = 1$, then $a \mid c$.

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

$$sac + tcb = c$$

but $a$ divides the second term of the sum since $a \mid bc$, and it obviously divides 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, $\gcd(p, b) = 1$. 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 $m = \gcd(a, b)$.

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

$$m \leq \gcd(a, b)$$

**STAFF NOTE**: If there is time, challenge students to prove that $m$ is a common divisor of $a$ and $b$ (and hence $m \leq \gcd(a, b)$) 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, $\gcd(a, b) \mid m$, which implies

$$\gcd(a, b) \leq m.$$