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

Problem 1. (a) Use the Pulverizer to find integers $x$, $y$ such that

$$x \cdot 50 + y \cdot 21 = \gcd(50, 21).$$

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>50</td>
<td>21</td>
<td>8</td>
<td>50 - 2 \cdot 21</td>
</tr>
<tr>
<td>21</td>
<td>8</td>
<td>5</td>
<td>21 - 2 \cdot 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>21 - 2 \cdot (50 - 2 \cdot 21)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-2 \cdot 50 + 5 \cdot 21</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>3</td>
<td>8 - 1 \cdot 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(50 - 2 \cdot 21) - 1 \cdot (-2 \cdot 50 + 5 \cdot 21)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 \cdot 50 - 7 \cdot 21</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>2</td>
<td>5 - 1 \cdot 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(-2 \cdot 50 + 5 \cdot 21) - 1 \cdot (3 \cdot 50 - 7 \cdot 21)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-5 \cdot 50 + 12 \cdot 21</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>1</td>
<td>3 - 1 \cdot 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(3 \cdot 50 - 7 \cdot 21) - 1 \cdot (-5 \cdot 50 + 12 \cdot 21)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8 \cdot 50 - 19 \cdot 21</td>
</tr>
</tbody>
</table>

(b) Now find integers $x', y'$ with $y' > 0$ such that

$$x' \cdot 50 + y' \cdot 21 = \gcd(50, 21)$$

Solution. since ($x, y$) = (8, -19) works, so does (8 - 21n, -19 + 50n) for any $n \in \mathbb{Z}$, so letting $n = 1$, we have

$$-13 \cdot 50 + 31 \cdot 21 = 1$$

Problem 2.

A number is perfect if it is equal to the sum of its positive divisors, other than itself. For example, 6 is perfect, because $6 = 1 + 2 + 3$. Similarly, 28 is perfect, because $28 = 1 + 2 + 4 + 7 + 14$. Explain why $2^{k-1}(2^k - 1)$ is perfect when $2^k - 1$ is prime.\(^1\)

---

\(^1\)Euclid proved this 2300 years ago. About 250 years ago, Euler proved the converse: every even perfect number is of this form (for a simple proof see [http://primes.utm.edu/notes/proofs/EvenPerfect.html](http://primes.utm.edu/notes/proofs/EvenPerfect.html)). As is typical in number theory, apparently simple results lie at the brink of the unknown. For example, it is not known if there are an infinite number of even perfect numbers or any odd perfect numbers at all.
Solution. If $2^k - 1$ is prime, then the only divisors of $2^{k-1}(2^k - 1)$ are:

$$1, \ 2, \ 4, \ \ldots, \ 2^{k-1}, \quad (1)$$

and

$$1 \cdot (2^k - 1), \ 2 \cdot (2^k - 1), \ 4 \cdot (2^k - 1), \ \ldots, \ 2^{k-2} \cdot (2^k - 1). \quad (2)$$

The sequence (1) sums to $2^k - 1$ (using the formula for a geometric series), and likewise the sequence (2) sums to $(2^{k-1} - 1) \cdot (2^k - 1)$. Adding these two sums gives $2^{k-1}(2^k - 1)$, so the number is perfect.  

Problem 3. (a) Let $m = 2^95^{24}11^717^{12}$ and $n = 2^37^{22}11^{211}13^117^919^2$. What is the gcd$(m,n)$? What is the least common multiple, lcm$(m,n)$, of $m$ and $n$? Verify that

$$\text{gcd}(m,n) \cdot \text{lcm}(m,n) = mn. \quad (3)$$

Solution.

$$g = 2^311^717^9, \quad l = 2^95^{24}7^{22}11^{211}13^117^{12}19^2$$

$$gl = 2^{12}5^{24}7^{22}11^{218}13^117^{21}19^2 = mn$$

(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 (3) 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$(m,n) \cdot \text{lcm}(m,n)$ 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 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$(a,b)$.

2It’s fun to notice the “computer science” proof that (1) sums to $2^k - 1$. The binary representation of $2^j$ is a 1 followed by $j$ 0’s, so expressed in binary, the sum is

$$1 + 10 + 100 + \cdots + 10 \cdots 0 = 1\ldots1.$$  

and the right hand expression is what you get by subtracting 1 from the binary representation of $2^k$.  

"5Staff Solutions to In-Class Problems Week 5, Mon."
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

\[
sac + tbc = c
\]

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

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