Math 522 Exam 2 Solutions

1. Use the Euclidean algorithm to find x, y satisfying $90x + 57y = 3$.

   We use long division five times as follows: $90 = 1\cdot57+33, 57 = 1\cdot33+24, 33 = 1 \cdot 24 + 9, 24 = 2 \cdot 9 + 6, 9 = 1 \cdot 6 + 3$. Now, we solve for 3, and repeatedly substitute in and simplify as follows: $3 = 1\cdot9-1\cdot6 = 1\cdot9-1(1\cdot24-2\cdot9) = 3\cdot9-1\cdot24 = 3(1\cdot33-1\cdot24)-1\cdot24 = 3\cdot33-4\cdot24 = 3\cdot33-4(1\cdot57-1\cdot33) = 7\cdot33-4\cdot57 = 7(1\cdot90-1\cdot57)-4\cdot57 = 7\cdot90-11\cdot57$. Hence $x = 7, y = -11$ satisfy the linear Diophantine equation.

2. For any nonzero integers a, b, prove that $\gcd(a, b) | \gcd(a + b, a - b) | \gcd(2a, 2b)$.
   BONUS: Characterize those a, b for which $\gcd(a, b) = \gcd(a + b, a - b)$.

   $\gcd(a, b) | \gcd(a+b, a-b)$: If $d|a$ and $d|b$, then $d|(a+b)$ and $d|(a-b)$ by the Divisibility Properties Theorem. Hence $\gcd(a, b) \in CD(a, b) \subseteq CD(a+b, a-b)$, so $\gcd(a, b) | \gcd(a + b, a - b)$ by the CD-PS Theorem.

   $\gcd(a + b, a - b)|2\gcd(a, b)$: If $d|a + b$ and $d|a - b$, then $d|(a + b + a - b)$ and $d|(a + b - a + b)$ by the Divisibility Properties Theorem. That is, $d|2a$ and $d|2b$. Hence, $\gcd(a + b, a - b) \in CD(a + b, a - b) \subseteq CD(2a, 2b)$, so $\gcd(a + b, a - b)| \gcd(2a, 2b)$ by the CD-PS Theorem.

   BONUS: We first prove the lemma that $\gcd(ac, bc) = c\gcd(a, b)$ for all nonzero integers a, b, c. This is proved with the last part of the D.P.T. $[CD(ac, bc) = cCD(a, b)]$. The proof proceeds in cases: if a, b are odd then $a + b, a - b$ are even and thus $2| \gcd(a + b, a - b)$ while $2 \nmid \gcd(a, b)$ and hence $\gcd(a, b) \neq \gcd(a + b, a - b)$. If one of a, b is odd and the other is even, then $a + b, a - b$ are odd, hence $\gcd(a + b, a - b)$ is odd. But $\gcd(a+b, a-b)| \gcd(2a, 2b) = 2\gcd(a, b)$, and so $\gcd(a+b, a-b)| \gcd(a, b)$ by Theorem 2-3 so they are equal (differ by a unit) by the D.P.T. Finally, if a, b are both even we may pull out all their common factors of 2 from the gcd, via: $\gcd(a, b) = \gcd(a+b, a-b)$ if and only if $\gcd(2\frac{a}{2}, 2\frac{b}{2}) = \gcd(2\frac{a+b}{2}, 2\frac{a-b}{2})$, if and only if $2\gcd(\frac{a}{2}, \frac{b}{2}) = 2\gcd(\frac{a+b}{2}, \frac{a-b}{2})$, if and only if $\gcd(\frac{a}{2}, \frac{b}{2}) = \gcd(\frac{a+b}{2}, \frac{a-b}{2})$. This reduces to one of the other two cases.

   To summarize the bonus: $\gcd(a, b) = \gcd(a + b, a - b)$ exactly when the highest power of 2 dividing a is different from the highest power of 2 dividing b. (otherwise $\gcd(a + b, a - b) = 2\gcd(a, b) = \gcd(2a, 2b)$)

3. High score=101, Median score=81, Low score=62