Math 223, Spring 2009
Midterm 1 Review Solutions

(1) Prove by induction.
   (a) For all $n \in \mathbb{N}$, we have $1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$.
   (b) For all $n \in \mathbb{N}$, $n \geq 4$, we have $2^n < n!$.

Solution:
   (a) The base case $n = 1$ clearly holds. If the statement is true for $n = k$, then

$$1^3 + 2^3 + \cdots + n^3 = \frac{k^2(k+1)^2}{4} + (k+1)^3 = (k+1)^2\frac{k^2+4k+4}{4} = \frac{(k+1)^2(k+2)^2}{4}.$$

   (b) The base case $n = 4$ clearly holds. If the statement is true for $n = k$, then

$$2^{k+1} = 2 \cdot 2^k < 2k! < (k+1)k! = (k+1)!.$$

(2) Let $a, b \in \mathbb{Z}$ and suppose $gcd(a, b) = 1$. Prove the following.
   (a) $gcd(a + b, a - b) = 1$ or 2.
   (b) $gcd(a + 2b, 2a + b) = 1$ or 3.
   (c) $gcd(a^n, b^n) = 1$ for all $n \in \mathbb{N}$.

Solution: We first prove the following
Lemma: Let $a, b \in \mathbb{Z}$ and let $g = gcd(a, b)$. Then for $n \in \mathbb{N}$, $gn = gcd(an, bn)$.

Proof: Let $c = gcd(an, bn)$. Note that $gn|an$ and $gn|bn$, so $gn \leq c$. Furthermore, we know by Linear Equation Theorem that there are $p, q \in \mathbb{Z}$ such that $pa + qb = g$. Therefore $pan + qbn = gn$. Since c divides the left side, $c|gn$. So $c \leq gn$ and thus we have $c = gn$ as desired.

   (a) Let $g = gcd(a + b, a - b)$. Note that g divides $(a + b) + (a - b) = 2a$ and $(a + b) - (a - b) = 2b$. So g divides $gcd(2a, 2b)$ (do you see why this is true?). By the above Lemma, $gcd(2a, 2b) = 2gcd(a, b) = 2$, so $g|2$, i.e. $g = 1$ or $g = 2$.
   (b) Let $g = gcd(a+2b, 2a+b)$. Note that g divides $2(2a+b)-(a+2b) = 3a$ and $2(a+2b)-(2a+b) = 3b$. So g divides $gcd(3a, 3b)$. By the above Lemma, $gcd(3a, 3b) = 3gcd(a, b) = 3$, so $g|3$, i.e. $g = 1$ or $g = 3$.
   (c) Suppose $g = gcd(a^n, b^n) > 1$. Then g has a prime factor p and thus $p|a^n$ and $p|b^n$. Hence $p|a$ and $p|b$ and it follows that $p|gcd(a, b) = 1$, which is a contradition.

(3) Let $a, b, c \in \mathbb{Z}$ and let $g = gcd(a, c)$. Prove that if $c|ab$, then $c|gb$.

Solution: If $c|ab$, then there are $m, n \in \mathbb{Z}$ such that $ma + nc = g$. If we multiply this equation by b, we get $mab + ncb = gb$. Since c divides ab, it divides the entire left side, and it thus divides gb.

(4) Decide if the following are true or false. If true, provide a proof. If false, provide a counterexample.
   (a) For all $k, n, r \in \mathbb{Z}$, $gcd(k, n) = gcd(k, n + rk)$.
   (b) For all $a, b, n \in \mathbb{Z}$, if $a^2|n$, $b^2|n$, and $a^2 \leq b^2$, then $a|b$.
   (c) For all $a, b, n \in \mathbb{N}$, if $a^n|b^n$, then $a|b$.

Solution:
   (a) This is true. Let $g = gcd(k, n)$ and let $c = gcd(k, n + rk)$. We want to show $g = c$. First, we know $g|k$ and $g|n$ and so $g|(n + rk)$. Therefore $g|c$. Also, we know that $c|k$ and $c|(n + rk)$. Therefore $c|n$ and so $c|g$. Thus $g = \pm c$ but since g and c are positive by definition, we have $g = c$.
   (b) This is false. Let $a = 2, b = 3$, and $n = 36$. Then $a^2|n$ and $b^2|n$ but $a \nmid b$.

(c) This is true. If $a^n|b^n$, then there exists a $k \in \mathbb{Z}$ such that $a^n k = b^n$, and so $k = (b/a)^n$, i.e. $\sqrt[n]{k}$ is rational. But this is impossible unless k is an nth power of some integer q. So $k = q^n$, and $q^n a^n = b^n$, so $b = \pm qa$. Therefore $a|b$.

(5) Kim Bottomly throws a party and orders apples and oranges at a total cost of \$8.39. If apples cost her 25 cents and oranges 18 cents each, how many of each type did she order?

Solution: We have the equation $25a + 18b = 839$. Euclidean Algorithm gives the solutions to $25a + 18b = gcd(25, 18) = 1$, which are found to be $(-5 + 18k, 7 - 25k)$, $k \in \mathbb{Z}$. The solutions to the equation $25a + 18b = 839$ are then given by pairs $(-5 \cdot 839 + 18k, 7 \cdot 839 - 25k)$ (why is this true?). Finding k such that both items in the pair are positive gives the answer we want.

(6) Kim Bottomly believes that she has 50 coins, all of which are pennies, dimes and quarters, with a total worth of 3 dollars. Determine whether her computations are possible.

Solution: We have the equations $p + d + q = 50$ and $p + 10d + 25q = 300$. Subtracting these equations, we get $9d + 24q = 250$ which has no solution since $gdc(9, 24) = 3$ which does not divide 250.

(7) Prove that, if a is an odd integer, then $a^2 \equiv 1 \pmod 8$. (Hint: All integers are of the form $4k + r$ where $k, r \in \mathbb{Z}$ and $0 \leq r < 4$. How about *odd* integers?)

Solution: If a is an odd integer, then $a \equiv 1, 3, 5,$ or $7 \pmod 8$. In each of these cases we have $a^2 \equiv 1 \pmod 8$.

(8) For $n \in \mathbb{N}$, suppose $n \equiv 3 \pmod 4$. Prove that n cannot be a sum of squares of two integers. (Hint: Use proof by contradiction.)

Solution: Suppose that there are $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = n$. Then $a^2 + b^2 \equiv 3 \pmod 4$. Now note that a square of an integer can only be congruent to 0 or 1 modulo 4. To see this, note that, for any even $c \in \mathbb{Z}$, c^2 has a factor of 4 so it is congruent to 0 mod 4, and if c is odd, then c^2 can be written as $4k + 1$ for some $k \in \mathbb{Z}$ and is thus congruent to 1 mod 4. Thus both a^2 and b^2 are congruent to 0 or 1 modulo 4, so their sum cannot be congruent to 3 modulo 4.

(9) Determine all values of x mod 301 such that $140x \equiv 133 \pmod{301}$. You will need to know that $gcd(140, 301) = 7$.

Solution: Since $7|133$, there are 7 solutions. To find them, first find the solutions to $140u + 301v = 7$. Before applying the Linear Equation Theorem, note that this equation simplifies since it can be divided by 7 to yield $20u + 43v = 1$. Euclidean Algorithm then provides a solution:

$$\begin{aligned} 43 &= 2 \cdot 20 + 3 \\ 20 &= 6 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Letting $a = 20$ and $b = 43$, we can repeat the above while solving for the remainder at each stage:

$$\begin{aligned} 3 &= b - 2a \\ 2 &= a - 6(b - 2a) = 13a - 6b \\ 1 &= (b - 2a) - (13a - 6b) = -15a + 7b. \end{aligned}$$

Thus a solution to $20u + 43v = 1$ is $(-15, 7)$ and all solutions to the original congruence are given by

$$x \equiv \frac{-15 \cdot 133}{7} + \frac{301}{7}k \pmod{301} = -285 + 43k \pmod{301} \equiv 16 + 43k \pmod{301} \quad \text{for} \quad k = 0, 1, ..., 6.$$

(10) Use Fermat's Little Theorem to do the following.
(a) Find the least residue of 1945^{12} modulo 11.
(b) Solve $x^{212} \equiv 6 \pmod 7$.

Solution:

(a) Since $gcd(11, 1945) = 1$, Fermat's Little Theorem gives $1945^{10} \equiv 1 \pmod{11}$. Then

$$1945^{12} \equiv 1945^{10}1945^2 \equiv 1945^2 \equiv 4 \pmod{11}.$$

(The last computation was done on a calculator.)

(b) We have

$$x^{212} = (x^6)^{35}x^2 \equiv x^2 \pmod{7},$$

so it suffices to solve $x^2 \equiv 6 \pmod{7}$. By inspection, we find that this equation has no solutions.