MATH 135 Algebra, Solutions to Term Test 2

[5] **1:** (a) Find all pairs of integers x and y such that $72x - 51y = 24$.

Solution: The Euclidean Algorithm gives

$$72 = 1 \cdot 51 + 21\ ,\quad 51 = 2 \cdot 21 + 9\ ,\quad 21 = 2 \cdot 9 + 3\ ,\quad 3 = 3 \cdot 3 + 0$$

so we have $\gcd(72, 51) = 3$, then Back-Substitution gives

$$1\ ,\quad -2\ ,\quad 5\ ,\quad -7$$

so we have $(72)(5) - (51)(7) = 3$. Multiply both sides by $\frac{24}{3} = 8$ to get $(72)(40) - (51)(56) = 24$. Thus one solution is $(x, y) = (40, 56)$. Note that $\frac{72}{3} = 24$ and $\frac{51}{3} = 17$ and so by the Linear Diophantine Equation Theorem, the general solution is

$$(x, y) = (40, 56) + k(17, 24)\ ,\quad k \in \mathbf{Z}\,.$$

[2] (b) Find all integers c with $0 \leq c \leq 30$ for which there exist integers x and y such that $35x + 56y = c$.

Solution: By the Linear Diophantine Equation Theorem, there exist integers x and y such that $35x+56y = c$ if and only if $\gcd(35, 56)\big|c$. By inspection, $\gcd(35, 56) = 7$, so the possible values of c are 0, 7, 14, 21 and 28.

[3] (c) Find the number of pairs of positive integers x and y such that $12x + 18y = 300$.

Solution: Divide both sides of the equation $12x + 18y = 300$ by 6 to get $2x + 3y = 50$. By inspection, $(x, y) = (25, 0)$ is one solution, and by the Linear Diophantine Equation Theorem, the general solution is

$$(x, y) = (25, 0) + k(3, -2)\ ,\quad k \in \mathbf{Z}\,.$$

We have $x > 0 \Longrightarrow 25+3k > 0 \Longrightarrow 3k > -25 \Longrightarrow k > -\frac{25}{3} \Longrightarrow k \geq -8$ and $y > 0 \Longrightarrow -2k > 0 \Longrightarrow k \leq -1$. Thus we need $-8 \leq k \leq -1$, so there are exactly 8 positive solutions.

[3] **2:** (a) Let $a = 10!$ and $b = 60^3$. Find the prime factorizations of $\gcd(a, b)$ and $\mathrm{lcm(a, b)}$.

Solution: We have $10! = (10)(9)(8)(7)(6)(5)(4)(3)(2) = (2 \cdot 5)(3^2)(2^3)(7)(2 \cdot 3)(5)(2^2)(3)(2) = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7^1$ and $60^3 = (2^2 \cdot 3 \cdot 5)^3 = 2^6 \cdot 3^3 \cdot 5^3$, and so

$$\gcd(10!, 60^3) = 2^6 \cdot 3^3 \cdot 5^2$$
$$\mathrm{lcm}(10!, 60^3) = 2^8 \cdot 3^4 \cdot 5^3 \cdot 7^1 \, .$$

[3] (b) Determine the number of positive integers n such that $n \big| 36000$ and $36000 \big| n^2$.

Solution: Note that $36000 = 2^5 \cdot 3^2 \cdot 5^3$. In order to have $n \big| 36000$ we must have $n = 2^i \cdot 3^j \cdot 5^k$ for some i, j, k with $0 \leq i \leq 5$, $0 \leq j \leq 2$ and $0 \leq k \leq 3$. Then we have $n^2 = 2^{2i} \cdot 3^{2j} \cdot 5^{2k}$, and so in order to have $36000 \big| n^2$ we need $5 \leq 2i$, $2 \leq 2j$ and $3 \leq 2k$, that is $i \geq 3$, $j \geq 1$ and $k \geq 2$. Thus $i \in \{3, 4, 5\}$, $j \in \{1, 2\}$, and $k \in \{2, 3\}$. Since there are 3 choices for i, 2 choices for j and 2 choices for k, there are $3 \cdot 2 \cdot 2 = 12$ such integers n.

[3] (c) Show that for all positive integers a and b, if $a^3 \big| b^2$ then $a \big| b$.

Solution: Let a and b be positive integers. Write $a = {p_1}^{k_1} {p_2}^{k_2} \cdots {p_m}^{k_m}$ and $b = {p_1}^{l_1} {p_2}^{l_2} \cdots {p_m}^{l_m}$ where the p_i are distinct primes and $k_i, l_i \geq 0$ for all i. Suppose that $a^3 \big| b^2$. Note that $a^3 = {p_1}^{3k_1} {p_2}^{3k_2} \cdots {p_m}^{3k_m}$ and $b^2 = {p_1}^{2l_1} {p_2}^{2l_2} \cdots {p_m}^{2l_m}$, so we must have $3k_i \leq 2l_i$ for all i, and hence $k_i \leq \frac{2}{3} l_i \leq l_i$ for all i. Thus $a \big| b$.

[1] (d) Show that there exist positive integers a and b such that $a^2 \big| b^3$ but $a \not| \, b$.

Solution: Let $a = 8$ and $b = 4$. Then $a^2 = 64 = b^3$ so $a^2 \big| b^3$ but $a \not| \, b$.

[2] **3:** (a) Find the smallest integer n with $n \geq 100$ such that $n \equiv 12 \pmod{17}$.

Solution: We have $n \equiv 12 \pmod{17} \iff n \in \{\cdots, -5, 12, 29, 46, 63, 80, 97, 114, \cdots\}$, so the smallest such value is $n = 114$.

[2] (b) If a clock now reads 7:00 pm, then what time did it read 500 hours ago?

Solution: Note that $500 = 20 \cdot 24 + 20$ so $-500 \equiv -20 \equiv 4 \pmod{24}$. Thus 500 hours ago, the clock read the same time that it read 20 hours ago, that is the same time that it will read in 4 hours, namely 11:00 pm.

[3] (c) Let $n = 4,001,005,003,002$. Find all primes p with $1 < p < 12$ such that $p \mid n$.

Solution: Since the final digit is 2, we have $2 \mid n$ and $5 \nmid n$. Since the sum of the digits is $4+1+5+3+2 = 15$ we have $3 \mid n$. Since the alternating sum of blocks of 3 digits is $4-1+5-3+2 = 7$ we have $7 \mid n$ and $11 \nmid n$ (by the result of Problem 5(c) on Assignment 7).

[3] (d) Show that if $n \equiv 4 \pmod{7}$ then n is not equal to the sum of two cubes.

Solution: We make a table of powers modulo 7.

x	0	1	2	3	4	5	6
x^2	0	1	4	2	2	4	1
x^3	0	1	1	6	1	6	6

We see that for all integers x, we have $x^3 \equiv 0$ or $\pm 1 \pmod{7}$. Similarly, for every integer y, we have $y^3 \equiv 0$ or $\pm 1 \pmod{7}$. Thus for all x and y we have

$$x^3 + y^3 \equiv 0+0, 0+1, 0-1, 1+0, 1+1, 1-1, -1+0, -1+1 \text{ or } -1-1 \pmod{7},$$

that is $x^3 + y^3 \equiv 0, \pm 1$ or $\pm 2 \pmod{7}$. Thus if n is a sum of two cubes we must have $n \equiv 0, \pm 1$ or $\pm 2 \pmod{7}$, so we cannot have $n \equiv 4 \pmod{7}$.

[2] **4:** (a) Define what it means for an integer p to be prime.

Solution: An integer p is prime when $p > 1$ and p has exactly two positive divisors (namely 1 and p).

[3] (b) State Fermat's Little Theorem.

Solution: Fermat's Little Theorem states that for all integers p and a, if p is a prime which does not divide a, then we have $a^{p-1} \equiv 1 \pmod{p}$.

[5] (c) Prove Euclid's Theorem, which states that there are infinitely many primes.

Solution: Suppose, for a contradiction, that there are only finitely many primes. Let $p_1, p_2, \cdots, p_l$ be a list of all of the primes. Let $n = p_1 p_2 \cdots p_l + 1$. Note that none of the primes p_i is a factor of n, because when n is divided by p_i the remainder is 1, not 0. This contradicts the fact that every integer $n > 1$ is either a prime or a product of primes (and hence must have a prime factor).

[5] **5:** (a) Find every element $x \in \mathbf{Z}_{175}$ such that $[77]x = [84]$.

Solution: To solve the related congruence $77x \equiv 84 \pmod{175}$ for $x \in \mathbf{Z}$, we consider the diophantine equation $77x + 175y = 84$. The Euclidean Algorithm gives

$$175 = 2 \cdot 77 + 21\ ,\quad 77 = 3 \cdot 21 + 14\ ,\quad 21 = 1 \cdot 14 + 7\ ,\quad 14 = 2 \cdot 7 + 0$$

so we have $\gcd(77, 175) = 7$. Then Back-Substitution gives

$$1\ ,\quad -1\ ,\quad 4\ ,\quad -9$$

so we have $(77)(-9)+(175)(4) = 7$. Multiply both sides by $\frac{84}{7} = 12$ to get $(77)(-108)+(175)(48) = 84$. Thus one solution to the congruence is $x = -108$. Note that $\frac{175}{7} = 25$, so by the Linear Congruence Theorem, the general solution to the congruence is $x \equiv -108 \equiv 17 \pmod{25}$. Thus for $x \in \mathbf{Z}_{175}$ we have $[77]x = [84]$ when

$$x = [17], [42], [67], [92], [117], [142] \text{ or } [167]$$

[5] (b) Find the remainder when $50^{50^{50}}$ is divided by 13.

Solution: We have $50 \equiv 11 \equiv -2 \pmod{13}$, so $50^{50^{50}} \equiv (-2)^{50^{50}} \pmod{13}$. By Fermat's Little Theorem, the list of powers of (-2) modulo 13 repeats every 12 terms, so we wish to find $50^{50} \pmod{12}$. We have $50 \equiv 2 \pmod{12}$, so $50^{50} \equiv 2^{50} \pmod{12}$. We make a list of powers of 2 modulo 12.

k	0	1	2	3	4
2^k	1	2	4	8	4

We see that the list repeats every two terms beginning with 2^2. We have $50 \equiv 0 \equiv 2 \pmod{2}$ and so $2^{50} \equiv 2^2 \equiv 4 \pmod{12}$. Thus

$$50^{50^{50}} \equiv (-2)^{50^{50}} \equiv (-2)^{2^{50}} \equiv (-2)^4 \equiv 16 \equiv 3 \pmod{13}.$$