PMATH 340 Elementary Number Theory, Solutions to the midterm test, Winter 2024

[10] **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

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

(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.

(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

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

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.

[10] **2:** (a) Find $\tau\big((22)!\big)$ and $\sigma(20520)$.

Solution: We have $(22)! = 2^{11+5+2+1}\cdot 3^{7+2}\cdot 5^4\cdot 7^3\cdot 11^2\cdot 13^1\cdot 17^1\cdot 19$ so that $\tau\big((22)!\big) = 20\cdot 10\cdot 5\cdot 4\cdot 3\cdot 2\cdot 2\cdot 2 = 96000$. We have $20520 = 2^3\cdot 3^3\cdot 5\cdot 19$ so that $\sigma(20520) = (1{+}2{+}4{+}8)(1{+}3{+}9{+}27)(1{+}5)(1{+}19) = 15\cdot 40\cdot 6\cdot 20 = 72000$.

(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 $0 \le i \le 5$, $0 \le j \le 2$ and $0 \le k \le 3$. 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 $5 \le 2i$, $2 \le 2j$ and $3 \le 2k$, that is $i \ge 3$, $j \ge 1$ and $k \ge 2$. 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.

(c) Prove 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 $k_i, l_i \ge 0$ 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 $3k_i \le 2l_i$ for all i, and hence $k_i \le \frac{2}{3}l_i \le l_i$ for all i. Thus $a\big|b$.

(d) Prove that $\gcd\big(5^{98}+3, 5^{99}+1\big) = 14$.

Solution: Recall that if $a = qb + r$ then $\gcd(b,a) = \gcd(b,r)$. Since $(2^{99}+1) = (5)(2^{98}+3) - 14$, we have

$$\gcd\big(5^{98}+3, 5^{99}+1\big) = \gcd\big(5^{98}+3, -14\big) = \gcd\big(5^{98}+3, 14\big)\,.$$

Note that $2\big|(5^{98}+3)$ since 5^{98} is odd and 3 is odd. Also, by Fermat's Little Theorem the list of powers of 5 repeats every 6 terms modulo 7, and we have $98 = 2 \mod 6$, so $5^{98}+3 = 5^2+3 = 28 = 0 \mod 7$, that is $7\big|(5^{98}+3)$. Since $2\big|(5^{98}+3)$ and $7\big|(5^{98}+3)$, we have $14\big|(5^{98}+3)$, and hence $\gcd\big(5^{98}+3, 14\big) = 14$.

[10] **3:** (a) Find every element $x \in \mathbb{Z}_{175}$ such that $77x = 84$.

Solution: To solve the related congruence $77x = 84 \pmod{175}$ for $x \in \mathbb{Z}$, 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 $x = -108 = 17 \mod 25$. Thus for $x \in \mathbb{Z}_{175}$ we have $77x = 84$ when

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

(b) Solve the pair of congruences $x = 5 \mod 9$ and $10x = 6 \mod 28$.

Solution: By dividing all terms by 2 then multiplying both sides by 3, we see that

$$10x = 6 \mod 28 \iff 5x = 3 \mod 14 \iff x = 9 \mod 14\,.$$

To get $x = 5 \mod 9$ and $x = 9 \mod 14$ we must have $x = 5 + 9r$ and $x = 9 + 14s$ for some integers r and s, so we need $5 + 9r = 9 + 14s$, that is $9r - 14s = 4$. By inspection, one solution to this equation is $(r, s) = (2, 1)$, and so one solution for the pair of congruences is $x = 5 + 9r = 5 + 9 \cdot 2 = 23$. Note that $9 \cdot 14 = 126$, so by the Chinese Remainder Theorem, the general solution is

$$x = 23 \mod 126\,.$$

(c) Prove that for all $n \in \mathbb{Z}$, if $n = 4 \mod 7$ 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

Thus for all $x, y \in \mathbb{Z}_7$ we have $x \in \{0, \pm 1\}$ and similarly $y \in \{0, \pm 1\}$, and hence

$$x^3 + y^3 \in \big\{0{+}0\,,\ 0{\pm}1\,,\ {\pm}1{+}0\,,\ {\pm}1{\pm}1\big\} = \big\{0, \pm 1, \pm 2\big\} = \{0, 1, 2, 5, 6\} \text{ in } \mathbb{Z}_7.$$

It follows that for every $x, y \in \mathbb{Z}$ we have $x^3 + y^3 \neq 4 \mod 7$ (and also $x^3 + y^3 \neq 3 \mod 7$).

[10] **4:** (a) Let $n = 16{,}000$. Find the smallest $k \in \mathbb{Z}^+$ such that $a^k = 1$ for every $a \in U_n$.

Solution: Note that $16000 = 2^7 \cdot 5^3$ and so the smallest such $k \in \mathbb{Z}^+$ is

$$k = \lambda(n) = \text{lcm}\big(\lambda(2^7), \lambda(5^3)\big) = \text{lcm}\big(2^5\,,\,5^3 - 5^2\big) = \text{lcm}(32, 100) = 800.$$

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

Solution: We have $50 = 11 = -2 \mod 13$, so $50^{50^{50}} = (-2)^{50^{50}} \mod 13$. By Fermat's Little Theorem, the list of powers of (-2) modulo 13 repeats every 12 terms, so we wish to find $50^{50} \mod 12$. We have $50 = 2 \mod 12$, so $50^{50} = 2^{50} \mod 12$. 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 $50 = 0 = 2 \mod 2$ and so $2^{50} = 2^2 = 4 \mod 12$. Thus

$$50^{50^{50}} = (-2)^{50^{50}} = (-2)^{2^{50}} = (-2)^4 = 16 = 3 \mod 13.$$

(c) With the help of the following list of powers of 5 mod 23, solve $11\,x^{18} = 15 \mod 23$.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
5^k	1	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14	1

Solution: Note that $x = 0$ is not a solution. For $x \neq 0$ we can write $x = 5^k$. Then

$$\begin{aligned} 11\,x^{18} = 15 \mod 23 &\iff 5^9\,5^{18\,k} = 5^{17} \mod 23 \\ &\iff 5^{18\,k} = 5^8 \mod 23 \\ &\iff 18\,k = 8 \mod 22 \\ &\iff 9\,k = 4 \mod 11 \\ &\iff k = 9 \mod 11 \\ &\iff k = 9 \text{ or } 20 \mod 22 \\ &\iff x = 5^k = 11 \text{ or } 12 \mod 23\,. \end{aligned}$$