Exam 2017-03-08; SOLUTIONS

1. We use the same method of presentation as in MNZ p. 218 (top).

(a).

$$\begin{pmatrix} 24 & 15 & -25 & 2 \\ 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{pmatrix} \to \begin{pmatrix} -6 & 15 & 5 & 2 \\ 1 & 0 & 0 & \\ -2 & 1 & 2 & \\ 0 & 0 & 1 & \end{pmatrix} \to \begin{pmatrix} -1 & 0 & 5 & 2 \\ 1 & 0 & 0 & \\ 0 & -5 & 2 & \\ 1 & -3 & 1 & \end{pmatrix}$$

$$\to \begin{pmatrix} -1 & 0 & 0 & 2 \\ 1 & 0 & 5 & \\ 0 & -5 & 2 & \\ 1 & -3 & 6 & \end{pmatrix}$$

Answer: $(x, y, z) = (-2 + 5s, -5t + 2s, -2 - 3t + 6s)$, $t, s \in \mathbb{Z}$.

(b). There are no solutions, since $\gcd(21, 14, -56) = 7$ does not divide 2.

2. (a) The prime factorization of 125 is $125 = 5^3$.

Set $f(X) = X^3 + X^2 + 3 \in \mathbb{Z}[X]$. By testing all five elements of $\mathbb{Z}_5$, we find that there are exactly two solutions to $f(X) \equiv 0 \bmod 5$, namely $X \equiv 1$ and $X \equiv 2 \bmod 5$. We have $f'(X) = 3X^2 + 2X$ and $f'(1) = 5 \equiv 0 \bmod 5$ and $f'(2) = 16 \equiv 1 \bmod 5$. Hence by Hensel's Lemma, $2 \bmod 5$ lifts to a unique solution modulo 25 and then to a unique solution mod 125, whereas $1 \bmod 5$ lifts to either 0 or 5 solutions $\bmod 25$. We compute $f(1) = 5 \not\equiv 0 \bmod 25$; hence in fact $1 \bmod 5$ lifts to 0 solutions $\bmod 25$. It follows that the given equation in $\mathbb{Z}_{125}$ has exactly one solution, namely the unique lift of the solution $2 \bmod 5$. To determine this lift, let $t \bmod 5$ be the unique solution to $f'(2)t \equiv -f(2)/5 \bmod 5$, i.e. $t \equiv -15/5 = -3 \bmod 5$; then the formula in Hensel's Lemma says that $b = 2 + 5 \cdot (-3) = -13 \equiv 12$ is the unique lift $\bmod 25$ of the solution $2 \bmod 5$. Next, to determine the lift modulo 125, let $t \bmod 5$ be the unique solution to $f'(12)t \equiv -f(12)/5^2 \bmod 5$, i.e. $t = 75 \equiv 0 \bmod 5$; then the formula in Hensel's Lemma says that $b = 12 + 25 \cdot 0 \equiv 12 \bmod 125$ is the unique lift $\bmod 125$ of the solution $12 \bmod 25$.

Answer: There is exactly one zero, namely $\overline{12}$.

(b) The prime factorization of 221 is $221 = 13 \cdot 17$. Note that $X^2 - 3X = (X-3)X$ in $\mathbb{Z}[X]$; hence we can immediately solve the congruence equation modulo 13 and modulo 17. Indeed, if $(X-3)X \equiv 0 \bmod 13$ then $X - 3$ or X must be divisible by 13, i.e. $X \equiv 0$ or $3 \bmod 13$. Similarly, the two solutions to $(X-3)X \equiv 0 \bmod 17$ are $x \equiv 0$ or $3 \bmod 17$.

Now we use the Chinese Remainder Theorem to determine all the solutions $\bmod 221$. We first seek $a, b \in \mathbb{Z}$ so that $13a + 17b = 1$; we find $a = 4$, $b = -3$ by simple testing (or using Euclid's Algorithm). From this we find the number $13 \cdot 4 = 52$ which is $\equiv 0 \bmod 13$ and $\equiv 1 \bmod 17$, and we also find the number $17 \cdot (-3) = -51$ which is $\equiv 1 \bmod 13$ and $\equiv 0 \bmod 17$. Hence for any $x, y \in \mathbb{Z}$, the unique integer $\bmod 221$ which is $\equiv x \bmod 13$ and $\equiv y \bmod 17$ equals $52x - 51y$. Applying this to the solutions of the given equation mod 13 and mod 17, we see that there are the following four solutions mod 221:

$$0 \cdot 52 + 0 \cdot (-51) = 0; \qquad 3 \cdot 52 + 0 \cdot (-51) = 156;$$
$$0 \cdot 52 + 3 \cdot (-51) = 153 \equiv 68; \qquad 3 \cdot 52 + 3 \cdot (-51) = 3.$$

Answer: $\overline{0}$, $\overline{3}$, $\overline{68}$ and $\overline{156}$.

3. (a) 607 is a prime, while $435 = 3 \cdot 5 \cdot 29$, and we compute

$$\left(\frac{435}{607}\right) = \left(\frac{3}{607}\right) \cdot \left(\frac{5}{607}\right) \cdot \left(\frac{29}{607}\right) = \left(-\left(\frac{607}{3}\right)\right) \cdot \left(\frac{607}{5}\right) \cdot \left(\frac{607}{29}\right)$$

$$= -\left(\frac{1}{3}\right) \cdot \left(\frac{2}{5}\right) \cdot \left(\frac{-2}{29}\right) = (-1) \cdot (-1) \cdot \left(\frac{2}{29}\right) = (-1) \cdot (-1) \cdot (-1) = -1.$$

Answer: No.

(b) Since $435 = 3 \cdot 5 \cdot 29$, $\overline{616}$ is a square in $\mathbb{Z}_{435}$ iff it is a square in $\mathbb{Z}_3$ and in $\mathbb{Z}_5$ and in $\mathbb{Z}_{29}$. We compute:

$$\left(\frac{616}{3}\right) = \left(\frac{1}{3}\right) = 1;$$

$$\left(\frac{616}{5}\right) = \left(\frac{1}{5}\right) = 1;$$

$$\left(\frac{616}{29}\right) = \left(\frac{7}{29}\right) = \left(\frac{29}{7}\right) = \left(\frac{1}{7}\right) = 1.$$

Hence $\overline{616}$ is a square in each of $\mathbb{Z}_3$, $\mathbb{Z}_5$ and $\mathbb{Z}_{29}$, and hence also in $\mathbb{Z}_{435}$.

Answer: Yes.

4. (a) $p = 29$ is a prime and $\phi(p) = p - 1 = 28 = 2^2 \cdot 7$. Let h be the order of $\overline{2}$ in $\mathbb{Z}_{29}$. By Fermat's Little Theorem, $\overline{2}^{28} = \overline{1}$; hence $h \mid 28$. Therefore, if $h \neq 28$, then we must have $h \mid 14$ or $h \mid 4$ and this would imply $\overline{2}^{14} = \overline{1}$ or $\overline{2}^{4} = \overline{1}$. Hence if we check that $\overline{2}^{14} \neq \overline{1}$ and $\overline{2}^{4} \neq \overline{1}$ then it follows that $h = 28$ and therefore that $\overline{2}$ is a primitive root in $\mathbb{Z}_{29}$. We compute in $\mathbb{Z}_{29}$:

$$\overline{2}^4 = \overline{16};$$
$$\overline{2}^6 = \overline{64} = \overline{6};$$
$$\overline{2}^8 = (\overline{16})^2 = \overline{256} = \overline{24} = \overline{-5};$$
$$\overline{2}^{14} = \overline{2}^6 \cdot \overline{2}^8 = \overline{6} \cdot (-\overline{5}) = -\overline{30} = -\overline{1}.$$

Hence $h = 28$, and we have proved that $\overline{2}$ is a primitive root in $\mathbb{Z}_{29}$.

(b) Note that if $x \in \mathbb{Z}_{29}$ satisfies $x^{64} = \overline{16}$ then $x \neq \overline{0}$ and thus $x \in \mathbb{Z}_{29}^{\times}$. Hence since $\overline{2}$ is a primitive root, there is some $j \in \mathbb{Z}$ (uniquely determined mod 28) such that $x = \overline{2}^j$. Now:

$$x^{64} = \overline{16} \Leftrightarrow (\overline{2}^j)^{64} = \overline{2}^4 \Leftrightarrow \overline{2}^{64j} = \overline{2}^4 \Leftrightarrow 64j \equiv 4 \bmod 28 \Leftrightarrow 16j \equiv 1 \bmod 7$$
$$\Leftrightarrow 2j \equiv 1 \bmod 7 \Leftrightarrow 4 \cdot 2j \equiv 4 \bmod 7 \Leftrightarrow j \equiv 4 \bmod 7$$
$$\Leftrightarrow j \equiv 4 \text{ or } 11 \text{ or } 18 \text{ or } 25 \bmod 28.$$

Hence our equation has exactly four zeros in $\mathbb{Z}_{29}$, namely $\overline{2}^4$, $\overline{2}^{11}$, $\overline{2}^{18}$ and $\overline{2}^{25}$. We compute:

$$\overline{2}^4 = \overline{16};$$
$$\overline{2}^7 = \overline{128} = \overline{12};$$
$$\overline{2}^{11} = \overline{2}^4 \cdot \overline{2}^7 = \overline{16} \cdot \overline{12} = \overline{192} = \overline{18};$$
$$\overline{2}^{18} = \overline{2}^{11} \cdot \overline{2}^7 = \overline{18} \cdot \overline{12} = \overline{216} = \overline{13};$$
$$\overline{2}^{25} = \overline{2}^{18} \cdot \overline{2}^7 = \overline{13} \cdot \overline{12} = \overline{156} = \overline{11}.$$

Answer: $\overline{11}$, $\overline{13}$, $\overline{16}$, $\overline{18}$.

5. The equation is homogeneous; hence it suffices to prove that there does not exist any *primitive* solution, i.e. a solution with $\gcd(x, y, z) = 1$. (Detailed proof of this claim: Assume that $\langle x, y, z\rangle$ is any integer solution to the equation, $\langle x, y, z\rangle \neq \langle 0, 0, 0\rangle$. Let $d = \gcd(x, y, z) \in \mathbb{Z}^+$. Then $\langle x/d, y/d, z/d\rangle$ is a primitive solution to the equation! Hence, if there does not exist any primitive solution to the equation, then there does not exist any integer solution at all except $\langle x, y, z\rangle = \langle 0, 0, 0\rangle$.)

Assume now that $\langle x, y, z\rangle$ is a primitive solution to the equation. Considering the equation modulo 7 we then have $5x^3 \equiv 11z^3 \bmod 7$, or equivalently (multiplying by $\overline{5}^{-1} = \overline{3} \in \mathbb{Z}_7^\times$): $x^3 \equiv -2z^3 \bmod 7$. Assume first that $7 \nmid z$. Then also $x^3 \equiv -2z^3 \not\equiv 0 \bmod 7$ and thus $7 \nmid x$. Therefore, by Fermat's Little Theorem, $x^6 \equiv z^6 \equiv 1 \bmod 7$. Hence if we raise the relation $x^3 \equiv -2z^3 \bmod 7$ to the power 2, we obtain $1 \equiv (-2)^2 \bmod 7$, i.e. $1 \equiv 4 \bmod 7$. This is a contradiction! Hence we must in fact have $7 \mid z$. Then $x^3 \equiv -2z^3 \equiv 0 \bmod 7$ and thus $7 \mid x$. It follows that both $5x^3$ and $11z^3$ are divisible by 7^3, and thus from the original equation we have $7y^3 \equiv 11z^3 - 5x^3 \equiv 0 \bmod 7^3$. This implies $y^3 \equiv 0 \bmod 7^2$ and hence $7 \mid y$. Hence $x \equiv y \equiv z \equiv 0 \bmod 7$, contradicting the assumption that $\langle x, y, z\rangle$ is a primitive solution. Hence there are no primitive solutions to the equation! $\square$

6. (a). We follow the algorithm from Lecture 12. Note that if we set $d = 7$, $u_0 = 0$, $v_0 = 1$, then $\sqrt{7} = \frac{u_0+\sqrt{d}}{v_0}$ and $v_0 \mid d - u_0^2$. Next we compute a_j for $j \geq 0$ and u_j, v_j for $j \geq 1$ using the recursion formulas $a_j = \left[\frac{u_j+\sqrt{d}}{v_j}\right]$, $u_{j+1} = a_j v_j - u_j$, $v_{j+1} = (d - u_{j+1}^2)/v_j$. We get:

j	0	1	2	3	4	5
u_j	0	2	1	1	2	2
v_j	1	3	2	3	1	3
a_j	2	1	1	1	4	

Thus $\sqrt{7} = \langle 2, \overline{1, 1, 1, 4} \rangle$.

We compute the convergents using the formulas $h_{-2} = 0$, $h_{-1} = 1$, $h_j = a_j h_{j-1} + h_{j-2}$ and $k_{-2} = 1$, $k_{-1} = 0$, $k_j = a_j k_{j-1} + k_{j-2}$.

j	-2	-1	0	1	2	3	4
a_j			2	1	1	1	4
h_j	0	1	2	3	5	8	
k_j	1	0	1	1	2	3	

Answer: $\sqrt{7} = \langle 2, \overline{1, 1, 1, 4} \rangle$, and the first four convergents are $\frac{h_0}{k_0} = \frac{2}{1}$, $\frac{h_1}{k_1} = \frac{3}{1}$, $\frac{h_2}{k_2} = \frac{5}{2}$, $\frac{h_3}{k_3} = \frac{8}{3}$.

(b). Since $\sqrt{7} = \langle 2, \overline{1, 1, 1, 4} \rangle$ with period $r = 4$, the first solution is given by $\langle x, y \rangle = \langle h_{r-1}, k_{r-1} \rangle = \langle 8, 3 \rangle$. Computing $(8 + 3\sqrt{7})^2 = 127 + 48\sqrt{7}$ and $(8 + 3\sqrt{7})^3 = (127 + 48\sqrt{7})(8 + 3\sqrt{7}) = 2024 + 765\sqrt{7}$ we find two more solutions: $\langle 127, 48 \rangle$ and $\langle 2024, 765 \rangle$.

Answer: $\langle 8, 3 \rangle$ and $\langle 127, 48 \rangle$ and $\langle 2024, 765 \rangle$.

(c). **Answer:** No, since $\langle 2, \overline{1, 1, 1, 4} \rangle$ has even period $r = 4$.

7. (This is MNZ p. 192, Problem 20.)

Recall that $\Omega(n) := \sum_{p|n} \mathrm{ord}_p(n)$; hence $\Omega(nm) = \Omega(n) + \Omega(m)$ for any $n, m \in \mathbb{Z}^+$, and so $\lambda(nm) = \lambda(n)\lambda(m)$ for any $n, m \in \mathbb{Z}^+$, i.e. λ is totally multiplicative as desired. Now set $F(n) := \sum_{d|n} \lambda(d)$. Then F is multiplicative by Theorem 2 from Lecture #8 (= Thm 4.4 in MNZ = Thm. 16.2 in LL). Note also $F(p^\alpha) = \sum_{j=0}^{\alpha} (-1)^j$, and this is 1 if α is even but 0 if α is odd. Hence, using the fact that F is multiplicative, for an arbitrary positive integer $n = \prod_p p^\alpha$ we have

$$F(n) = \prod_p F(p^\alpha) = \prod_p \left\{ \begin{matrix} 1 & \text{if } \alpha \text{ is even} \\ 0 & \text{if } \alpha \text{ is odd} \end{matrix} \right\} = \begin{cases} 1 & \text{if } n \text{ is a perfect square} \\ 0 & \text{otherwise.} \end{cases}$$

(In the last step we used the fact that $n = \prod_p p^\alpha$ is a perfect square iff the exponent α is even for every prime p.)

8. (This is MNZ, problem 42 on p. 74.)

For any positive integer n we have

$$\frac{n}{\phi(n)} = \frac{1}{\prod_{p|n}(1 - p^{-1})} = \prod_{p|n} \frac{p}{p-1},$$

and $\phi(n) \mid n$ iff the above ratio is an integer. Assume now that this holds. Let A be the set of primes dividing n; thus now $\prod_{p\in A} \frac{p}{p-1} \in \mathbb{Z}$, i.e.

$$\prod_{p\in A}(p-1) \;\Big|\; \prod_{p\in A} p \tag{1}$$

Assume that there is a prime $q > 3$ in the set A. Then $q - 1$ divides $\prod_{p\in A} p$; but clearly $\mathrm{ord}_2(\prod_{p\in A} p) \le 1$; hence $q - 1 = 2u$ for some odd integer $u \ge 3$. Let q' be a prime factor of u; then $2 < q' < q$, and (1) implies that $q' \in A$. But then (1) implies $\mathrm{ord}_2(\prod_{p\in A} p) \ge 2$, a contradiction! Hence A cannot contain any prime $q > 3$. We also note that if $3 \in A$ then (1) forces $2 \in A$. Hence the only possibilities for A are: $A = \emptyset$, $A = \{2\}$ and $A = \{2, 3\}$. Hence the only possibilities for n are: $n = 1$ or 2^j or $2^j 3^k$ with $j, k \in \mathbb{Z}^+$. Conversely one verifies that $\phi(n) \mid n$ holds for all these n. □