MATH 235: Assignment 5 Solutions

1.1: Writing $N = n_0 + 10n_1 + \ldots + 10^k n_k$, we can reduce $\mod 3$ and using that fact that 10 is congruent with $1 \mod 3$, we conclude that

$$N \equiv n_0 + 1 \times n_1 + 1^2 \times n_2 + \ldots + 1^k \times n_k.$$

Clearly then $N \equiv 0 \mod 3$ iff the sum of its digits are also congruent to 0 mod 3.

1.2: Proceeding similarly to (1.1), we notice that $10 \equiv -1 \mod 11$. It follows that

$$N \equiv n_0 + (-1)n_1 + (-1)^2 n_2 + \ldots + (-1)^k n_k.$$

We conclude easily that N is congruent to $0 \mod 11$ iff the alternating sum of its digits are.

1.3: Notice that $M = (N - n_0)/10$. Multiply both sides by 10 and reduce modulo 7 to get $10 * M \equiv (N - n_0)$. Multiplying both sides of this equation by -2 and using the fact that $-20 \equiv 1 \mod 7$ we get $M \equiv -2N + 2n_0$. Rearrange to get $M - 2n_0 \equiv -2N$. Clearly if N is divisible by 7, then so is the left hand side, and likewise, if $M - 2n_0$ is divisible by 7, then so is N, since $(-2, 7) = 1$.

2: In a similar fashion to (1.1) and (1.2) above, it is easy to see that if $N = n_0 + 10n_1 + \ldots + 10^k n_k$ then $N \equiv n_0 + n_1 + \ldots + n_k \mod 9$. Notice that summing digits repeatedly for any number other then 0 will eventually leave you with a result lying between 1 and 9 and these numbers make up all distinct residue classes modulo 9. It follows that if $x \equiv y \mod 9$ and neither are 0, then repeatedly summing the digits of x and repeatedly summing the digits of y will eventually lead to the same answer (namely their congruence class representative in $\{1 \ldots 9\}$. Since $A \times B = C$, obviously then $A \times B \equiv C \mod 9$ and so if multiplication is done correctly, the above argument shows that the sum of the digits of ab is equal to c. *Note of course that the reverse statement is NOT true.

3.1: $x^2 + x = x(x+1)$ so it is obvious that both $\overline{0}$ and $\overline{-1} = \overline{4}$ satisfy the equation. One can easily check that no other solutions exist (Or use problem (5) below).

3.2: Again it is obvious that $\overline{0}$ and $\overline{5}$ are solutions. One also checks directly that $\overline{2}, \overline{3}$ are also solutions and that there are no others.

3.3: One may apply the result from (5) below, or proceed as follows. We have the equation $x^2 + x = x(x+1) \equiv 0 \mod p$. If $\overline{a}$ satisfies the equivalence, we must have $p | a(a+1)$. Since p is a prime, it follows from the fundamental theorem of arithmetic that p divides either a or $a+1$. We can conclude immediately that $\overline{a}$ equals either $\overline{0}$ or $\overline{p-1}$.

4.1: Since $(12, 19) = 1$ we know there exists a unique solution to our linear equation of equivalence classes modulo 19. Looking mod 19, we note that $2 \equiv 2 + 19 \times 10 = 192 = 12(16)$. Hence $x = \overline{16}$.

4.2: Again (7,24) $= 1$, so there is a unique solution. $2 \equiv 2 + 4 \times 24 = 98 = 7(14)$. Therefore $x = \overline{14}$.

4.3: Again there is a unique solution. $1 \equiv 1 + 13 \times 50 = 651 = 31(21)$. Hence $x = \overline{21}$.

4.4: $1 \equiv 1 + 7 \times 97 = 680 = 34(20)$. Hence $\overline{x} = 20$.

4.5: $2 \equiv 2 + 4 \times 40 = 162 = 27(6)$. Hence $\overline{x} = 6$.

4.6: Note that (15,63) $= 3$ and $3 \not| 5$. Hence there are no solutions.

5: Proceeding as in the proof of the quadratic formula over $\mathbb{C}$, we "complete the square" on the left hand side of the equation $ax^2 + bx + c = 0$ to get

$$a(x^2 + ba^{-1}x) + c \pm b^2(4a)^{-1} = a(x + b(2a)^{-1})^2 + c - b^2(4a)^{-1} = 0.$$

Note that since p is a prime strictly greater then 2 and $a \neq \overline{0}$, the equivalence classes $2a$ and $4a$ both have inverses. Rearranging terms, we are lead to the equation $(x+b(2a)^{-1})^2 = b^2 4^{-1} a^{-2} - ca^{-1}$. Multiply both sides of the equation by $4a^2$ to get $(2ax+b)^2 = b^2 - 4ac$. If $b^2 - 4ac$ is not the square of a residue class modulo p, then clearly no valuation of x will solve the above equation. On the other hand, if $b^2 - 4ac$ is a square mod p, say $s^2 \equiv b^2 - 4ac$, then it is easy to see that $(-s)^2 \equiv b^2 - 4ac$ and that $\overline{s}$ and $\overline{-s}$ are the only 2 solutions to $u^2 = b^2 - 4ac \mod p$ (consider the proof in (3.3) of why there are only 2 solutions to $x^2 + x$). It follows in this case that $2ax + b = \pm s$ and so

$$x = (-b \pm s)(2a)^{-1} = (-b \pm \sqrt{b^2 - 4ac})(2a)^{-1}.$$

5.2: By the previous result, it suffices to show for which values of a the class $\overline{1 - 4a}$ has a square mod 7. It is easy to check directly that the only squares modulo 7 are $\overline{0}, \overline{1}, \overline{2}$ and $\overline{4}$. $1 - 4a$ attains one of these values precisely when $a \in \{\overline{0}, \overline{1}, \overline{2}, \overline{5}\}$.