PMATH 340 Number Theory, Solutions to the Exercises for Chapter 2

1: (a) Find the inverse of 178 in $\mathbf{Z}_{365}$.

Solution: We find s and t so that $178s + 365t = 1$ so that $178^{-1} = s$. The Euclidean Algorithm gives

$$\begin{aligned} 365 &= 2 \times 178 + 9 \\ 178 &= 19 \times 9 + 7 \\ 9 &= 1 \times 7 + 2 \\ 7 &= 3 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

so $\gcd(178, 365) = 1$, then back substitution gives $u_k = 1, -3, 4, -79, 162$, so $(178)(162) + (365)(-79) = 1$ and hence $178^{-1} = 162$.

(b) Solve the linear congruence $356\,x \equiv 28 \pmod{730}$.

Solution: We have $356\,x \equiv 28 \pmod{730} \iff 178\,x = 14 \pmod{365}$. Multiply by $178^{-1} = 162$ to get $x = 162 \cdot 14 = 2268 = 78 \pmod{365}$.

2: Solve the following system of linear equations in $\mathbf{Z}_{20}$.

$$\begin{aligned} x - 2y + 3z &= 1 \\ 2x + \ \ y + 4z &= -2 \\ x + 3y + 7z &= 5 \end{aligned}$$

Solution: We do some basic operations on the equations to get

$$\left(\begin{array}{ccc|c} 1 & -2 & 3 & 1 \\ 2 & 1 & 4 & -2 \\ 1 & 3 & 7 & 5 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & -2 & 3 & 1 \\ 0 & 5 & -2 & -4 \\ 0 & 5 & 4 & 4 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & -2 & 3 & 1 \\ 0 & 5 & -2 & -4 \\ 0 & 0 & 6 & 8 \end{array}\right)$$

The third equation has become $6z = 8$, and the solutions are $z = 8, 18$. Put $z = 8$ or 18 into the second equation $5y - 2z = -4$ to get $5y = 12$. This has no solution in $\mathbf{Z}_{20}$, so the given system has no solution.

3: Solve the following system of congruences.

$$x^2 \equiv x + 6 \pmod{10}$$
$$2x^3 \equiv 7 \pmod{9}$$
$$x \equiv 11 \pmod{24}$$

Solution: Modulo 10 we have

x	0	1	2	3	4	5	6	7	8	9
x^2	0	1	4	9	6	5	6	9	4	1
$x+6$	6	7	8	9	0	1	2	3	4	5

so $x^2 \equiv x+6 \pmod{10} \iff x \equiv 3$ or $8 \pmod{10} \iff x \equiv 3 \pmod{5}$. Modulo 9 we have

x	0	1	2	3	4	5	6	7	8
x^2	0	1	4	0	7	7	0	4	1
x^3	0	1	8	0	1	8	0	1	8
$2x^3$	0	2	7	0	2	7	0	2	7

so $2x^3 \equiv 7 \pmod{9} \iff x \equiv 2$, 5 or $8 \pmod{9} \iff x \equiv 2 \pmod{3}$. Thus we need to solve the 3 equations

$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{3}$$
$$x \equiv 11 \pmod{24}$$

By inspection, one solution to the first two of these equations is $x_0 = 8$, so by the C.R.T. the complete solution is $x \equiv 8 \pmod{15}$. Thus we need to solve the pair of equations

$$x \equiv 8 \pmod{15}$$
$$x \equiv 11 \pmod{24}$$

We need $x = 8 + 15k = 11 + 24l$ (1) for some k, l, so we solve $15k - 24l = 3$. Divide this equation by 3 to get $5k - 8l = 1$. By inspection, one solution is $(k_0, l_0) = (-3, -2)$. Put k_0 (or l_0) into (1) to get one solution $x_0 = 8 + 15k_0 = 8 - 45 = -37$. Also, $\operatorname{lcm}(15, 24) = 120$, so by the C.R.T the complete solution is $x \equiv -37 \pmod{120} \equiv 83 \pmod{120}$.

4: Solve $x^3+6x\equiv 43 \pmod{792}$.

Solution: By the CRT, we can instead solve the three equations

$$x^3+6x\equiv 43\equiv 3 \pmod 8$$
$$x^3+6x\equiv 43\equiv 7 \pmod 9$$
$$x^3+6x\equiv 43\equiv 10 \pmod{11}$$

Modulo 8 we have

x	0	1	2	3	4	5	6	7
x^2	0	1	4	1	0	1	4	1
x^3	0	1	0	3	0	5	0	7
x^3+6x	0	7	4	5	0	3	4	1

so the solution to the equation modulo 8 is $x\equiv 5 \pmod 8$. Modulo 9 we have

x	0	1	2	3	4	5	6	7	8
x^2	0	1	4	0	7	7	0	4	1
x^3	0	1	8	0	1	8	0	1	8
x^3+6x	0	7	2	0	7	2	0	7	2

so the solution to the equation modulo 9 is $x\equiv 1$, 4 or 7 $\pmod 9$, or equivalently $x\equiv 1 \pmod 3$. Modulo 11 we have

x	0	1	2	3	4	5	6	7	8	9	10
x^2	0	1	4	9	5	3	3	5	9	4	1
x^3	0	1	8	5	9	4	7	2	6	3	10
x^3+6x	0	7	9	1	0	1	10	0	10	2	4

so the solution to the equation modulo 11 is $x\equiv 6$ or $8 \pmod{11}$. So now we need to solve the 3 linear equations

$$x\equiv 5 \pmod 8$$
$$x\equiv 1 \pmod 3$$
$$x\equiv 6 \text{ or } 8 \pmod{11}$$

One solution to the first two of these is $x_0=13$, so by the C.R.T. the complete solution to the first 2 is $x\equiv 13 \pmod{24}$. And now, we only need to solve the 2 linear equations

$$x\equiv 13 \pmod{24}$$
$$x\equiv 6 \text{ or } 8 \pmod{11}$$

Case 1: if $x\equiv 6 \pmod{11}$ then we need $(*)$ $x=13+24k=6+11l$ for some k,l so we solve $11l-24k=7$. The E.A. gives $24=2\times 11+2$, $11=5\times 2+1$ and $2=2\times 1+0$ and then B.S. gives $u_k=1,-5,11$ showing that $(11)(11)-(24)(5)=1$. Multiply this equation by 7 to get one solution for k and l: $(k_0,l_0)=(35,77)$. Put $k_0=35$ (or $l_0=77$) into $(*)$ to get a solution for x: $x_0=6+11\times 77=853$. By the C.R.T the complete solution for x is $x\equiv 853 \pmod{264}\equiv 61 \pmod{264}$.

Case 2: if $x\equiv 8 \pmod{11}$ then we need $(**)$ $x=13+24k=8+11l$ for some k,l, so we solve $11k-24l=5$. We already used the E.A. and B.S. to show that $(11)(11)-(24)(5)=1$. Multiply this by 5 to get one solution for k and l: $(k_0,l_0)=(25,55)$. Put $k_0=25$ into $(**)$ to get one solution for x: $x_0=13+24\times 25=613$. By the C.R.T. the complete solution is $x\equiv 613 \pmod{264}\equiv 85 \pmod{264}$.

Thus the final answer is $x\equiv 61$ or $85 \pmod{264}$.

5: Let $n = p^k$ where p is prime and $k \geq 1$. Let $f(x) = x^3 + 2x^2 - x - 2 = (x-1)(x+1)(x+2)$. Determine the number of solutions in $\mathbf{Z}_n$ to the equation $f(x) = 0$. Express your answer in terms of p and k.

Solution: We consider several cases. When $p = 2$ and $k = 1$ so $n = 2$, there are 2 solutions to $f(x) = 0$ in $\mathbf{Z}_n$, namely $x = 0, 1$. When $p = 2$ and $k = 2$ so $n = 4$, there are 3 solutions to $f(x) = 0$ in $\mathbf{Z}_n$, namely $x = 1, 2, 3$. When $p = 2$ and $k \geq 3$ and $n = p^k$, notice that when $(x+2)$ is even, $(x-1)$ and $(x+1)$ are both odd, and when $(x+2)$ is odd, $(x-1)$ and $(x+1)$ are both even, and in this case exactly one of the two numbers $(x-1)$ and $(x+1)$ is a multiple of 4. Thus $2^k \big| (x-1)(x+1)(x+2) \iff \big(2^k \big| (x+2) \text{ or } 2^{k-1} \big| (x-1) \text{ or } 2^{k-1} \big| (x+1)\big)$, and so there are 5 solutions to $f(x) = 0$ in $\mathbf{Z}_n$, namely $x = -2, 1, 1 + 2^{k-1}, -1$ and $-1 + 2^{k-1}$.

When $p = 3$ and $k = 1$ so $n = 3$, there are 2 solutions to $f(x) = 0$ in $\mathbf{Z}_n$, namely $x = 1, 2$. When $p = 3$ and $k = 2$ so $n = 9$, there are 4 solutions to $f(x) = 0$ in $\mathbf{Z}_n$, namely $x = 1, 4, 7, 8$. When $p = 3$ and $k \geq 3$ and $n = p^k$, notice that when $(x+1)$ is a multiple of 3, neither $(x-1)$ nor $(x+2)$ can be a multiple of 3 and that $3 \big| (x-1) \iff 3 \big| (x+2)$ and in this case 9 can only divide one of the two numbers $(x-1)$ and $(x+2)$. Thus $3^k \big| (x-1)(x+1)(x+2) \iff \big(3^k \big| (x+1) \text{ or } 3^{k-1} \big| (x-1) \text{ or } 3^{k-1} \big| (x+2)\big)$, and so there are 7 solutions to $f(x) = 0$ in $\mathbf{Z}_n$, namely $x = -2, 1, 1 + 3^{k-1}, 1 + 2 \cdot 3^{k-1}, -2, -2 + 3^{k-1}$ and $-2 + 2 \cdot 3^{k-1}$.

Finally, when $p > 3$ and $k \geq 1$ and $n = p^k$, notice that p can only divide one of the three numbers $(x-1)$, $(x+1)$ and $(x+2)$, and so $p^k \big| (x-1)(x+1)(x+2) \iff \big(p^k \big| (x-1) \text{ or } p^k \big| (x+1) \text{ or } p^k \big| (x+2)\big)$, and so there are 3 solutions to $f(x) = 0$ in $\mathbf{Z}_n$, namely $x = 1, -1, -2$.