Solutions to MATH3411 Problems 60–67

60.

(a) $\phi(17) = 16$ and $\gcd(2, 17) = 1$, so by Euler's Theorem, $2^{16} \equiv 1 \pmod{17}$, so

$$2^{1001} = 2^{16\times 62+9} = \left(2^{16}\right)^{62}(2^4)^2 2 \equiv 1^{62}16^2 \times 2 \equiv (-1)^2 2 \equiv 2 \pmod{17}$$

(a) $\phi(100) = \phi(2^2)\phi(5^2) = 2 \times 20 = 40$ and $\gcd(3, 100) = 1$, so by Euler's Theorem, $3^{40} \equiv 1 \pmod{100}$, so

$$3^{1001} = 3^{40\times 25+1} = \left(3^{40}\right)^{25} 3 \equiv 1^{25} 3 \equiv 3 \pmod{100}$$

so the two last digits are "03".

61. First try to find a primitive root for $\mathbb{Z}_{11}$, first trying 2: its powers $2^1, \ldots, 2^{10}$ are

$$2, 4, 8, 5, 10, 9, 7, 3, 6, 1$$

and we see that 2 is a primitive root for $\mathbb{Z}_{11}$. (Here, we could reduce calculations by checking that $2^{\frac{11-1}{5}} = 2^2 \neq 1$ and $2^{\frac{11-1}{2}} = 2^5 \neq 1$, since the order of $\mathbb{U}_{11}$ is $10 = 2 \times 5$ which has prime factors 2 and 5.)
All $(\phi(\phi(11)) = 4)$ primitive roots for $\mathbb{Z}_{11}$ are now given by 2^i with $\gcd(i, 11 - 1) = \gcd(i, 10) = 1$; that is

$$2^1 = 1, \quad 2^3 = 8, \quad 2^7 = 7, \quad 2^9 = 6$$

Now try to find a primitive root for $\mathbb{Z}_{17}$, first trying 2: its powers $2^1, \ldots, 2^{16}$ are

$$2, 4, 8, 16, 15, 13, 9, 1, \ldots$$

We see that 2 is a not primitive root for $\mathbb{Z}_{17}$. (Here, it is enough just to test whether $2^{\frac{16}{2}} = 2^8 = 1$ or not, since the order of $\mathbb{U}_{17}$ is $16 = 2^4$ which just contains the single prime factor 2.)
Let us then try 3: its powers $3^1, \ldots, 3^{16}$ are

$$3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1$$

We see that 3 is a primitive root for $\mathbb{Z}_{17}$. (Again, we really just needed just check that $3^{\frac{17-1}{2}} = 3^8 \neq 1$.)
All $(\phi(\phi(11)) = 4)$ primitive roots for $\mathbb{Z}_{17}$ are now given by 3^i with $\gcd(i, 17 - 1) = \gcd(i, 16) = 1$;
that is the odd powers of 3:

$$3, 10, 5, 11, 14, 7, 12, 6$$

62.

(a) First use the Euclidean algorithm forwards (in $\mathbb{Z}$):

$$\begin{aligned} x^3+1 &= x\times(x^2+1)+(-x+1)\\ x^2+1 &= (-x-1)\times(-x+1)+2\\ -x+1 &= \frac{1}{2}(-x+1)\times 2+0 \end{aligned}$$

so a greatest common divisor of $f=x^3+1$ and $g=x^2+1$ is 2.
Scaling to get a monic polynomial gives us that $d=\gcd(f,g)=1$.
Now use the Euclidean algorithm backwards, letting $h=-x+1$:

$$\begin{aligned} 2 &= g-(-x-1)h\\ &= g-(-x-1)(f-xg)\\ &= (x+1)f+(-x^2-x+1)g \end{aligned}$$

Hence, $d=\gcd(f,g)=1=af+bg$ for $a=\frac{1}{2}(x+1)$ and $b=\frac{1}{2}(-x^2-x+1)$.

(b) First use the Euclidean algorithm forwards (in $\mathbb{Z}_2$):

$$\begin{aligned} x^3+1 &= x\times(x^2+1)+(x+1)\\ x^2+1 &= (x+1)\times(x+1)+0 \end{aligned}$$

so $d=\gcd(f,g)=x+1$.
Now use the Euclidean algorithm backwards:

$$x+1=f-xg$$

Hence, $d=\gcd(f,g)=x+1=af+bg$ for $a=1$ and $b=-x$.

(c) First use the Euclidean algorithm forwards (in $\mathbb{Z}_3$):

$$\begin{aligned} x^3-x^2-1 &= x\times(x^2-x+1)+(-x-1)\\ x^2-x+1 &= (-x+2)\times(-x-1)+0 \end{aligned}$$

so a greatest common divisor of $f=x^3+1$ and $g=x^2+1$ is $-x-1$.
Scaling to get a monic polynomial gives us that $d=\gcd(f,g)=x+1$.
Now use the Euclidean algorithm backwards:

$$-x-1=f-xg$$

Hence, $d=\gcd(f,g)=x+1=af+bg$ for $a=-1$ and $b=x$.

63.

(a) In $\mathbb{Z}_2$ and modulo x^2+x+1,

$$\begin{aligned} x^5+x^2+1 &= x^5+x^2+1+x^3(x^2+x+1) \\ &= x^4+x^3+x^2+1 \\ &= x^4+x^3+x^2+1+x^2(x^2+x+1) \\ &= 1 \end{aligned}$$

(b) In $\mathbb{Z}_3$ and modulo x^2+x+1,

$$\begin{aligned} x^5+x^2+1 &= x^5+x^2+1-x^3(x^2+x+1) \\ &= -x^4-x^3+x^2+1 \\ &= -x^4-x^3+x^2+1+x^2(x^2+x+1) \\ &= 2x^2+1 \\ &= 2x^2+1+(x^2+x+1) \\ &= x+2 \end{aligned}$$

64.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

both

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

$\mathbb{Z}_2/\langle x^2+x+1\rangle$

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

$\mathbb{Z}_2/\langle x^2+1\rangle$

Every non-zero element in $\mathbb{Z}_2/\langle x^2+x+1\rangle$ has an inverse and is therefore a unit,
in contrast to the element $x+1$ in $\mathbb{Z}_2/\langle x^2+1\rangle$.
Therefore, $\mathbb{Z}_2/\langle x^2+x+1\rangle$ is a field and $\mathbb{Z}_2/\langle x^2+1\rangle$ is not.

65. Since $m = x^4+x^2+x+1$ has 1 as a root in $\mathbb{Z}_2$, it is divisible by $x-1$ and is therefore not irreducible.
Hence, $\mathbb{Z}_2/\langle x^4+x^2+x+1\rangle$ is not a field.

Let us see whether m is irreducible in $\mathbb{Z}_3$.
We first note that $m(0)=m(1)=1$ and $m(2)=2$, so m has no roots and thus no linear factor.
Suppose that

$$m = x^4+x^2+x+1 = (x^2+ax+b)(x^2+cx+d) = x^4+(a+c)x^3+(b+ac+d)x^2+(ad+bc)x+bd$$

Comparing terms, we see that $c=-a$ and that $b=d^{-1}=d\neq 0$ (in $\mathbb{Z}_3$).
Therefore, $ad+bc = ad-da = 0 \neq 1$, a contradiction.
Therefore, m has no linear or quadratic divisors in $\mathbb{Z}_3$ and must be irreducible.
Hence, $\mathbb{Z}_2/\langle x^4+x^2+x+1\rangle$ is a field.

66.

(a) Here, we have that $\alpha^3 = -\alpha - 1 = \alpha + 1$.

i	0	1	2	3	4	5	6	7
α^i	1	α	α^2	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 1$	$\alpha^2 + 1$	1

The element α is primitive, so all of the primitive elements of $\mathbb{Z}_2/\langle x^3 + x + 1\rangle$ are given by α^i where $\gcd(i, 7) = 1$; that is all of the 6 elements listed above: $\alpha, \dots, \alpha^2 + 1$.

(b) Here, $\alpha^4 = \alpha^3 + \alpha^2 + \alpha + 1$.
Since $\alpha^5 = 1$, $\operatorname{ord}(\alpha) \leq 5 < 8$, so α is not primitive in $\mathbb{Z}_2/\langle x^4 + x^3 + x^2 + x + 1\rangle$.
Let us therefore consider $\gamma = \alpha + 1$ for instance:

$\gamma^0 = 1$	$\gamma^8 = \gamma^3 + \gamma^2 + \gamma = \alpha^3 + 1$
$\gamma^1 = \alpha + 1$	$\gamma^9 = \gamma^2 + 1 = \alpha^2$
$\gamma^2 = \alpha^2 + 1$	$\gamma^{10} = \gamma^3 + \gamma = \alpha^3 + \alpha^2$
$\gamma^3 = \alpha^3 + \alpha^2 + \alpha + 1$	$\gamma^{11} = \gamma^3 + \gamma^2 + 1 = \alpha^3 + \alpha + 1$
$\gamma^4 = \alpha^3 + \alpha^2 + \alpha = \gamma^3 + 1$	$\gamma^{12} = \gamma + 1 = \alpha$
$\gamma^5 = \gamma^3 + \gamma + 1 = \alpha^3 + \alpha^2 + 1$	$\gamma^{13} = \gamma^2 + \gamma = \alpha^2 + \alpha$
$\gamma^6 = \gamma^3 + \gamma^2 + \gamma + 1 = \alpha^3$	$\gamma^{14} = \gamma^3 + \gamma^2 = \alpha^3 + \alpha$
$\gamma^7 = \gamma^2 + \gamma + 1 = \alpha^2 + \alpha + 1$	$\gamma^{15} = 1$

The element γ is primitive, so all of the primitive elements of $\mathbb{Z}_2/\langle x^4 + x^3 + x^2 + 1\rangle$ are given by α^i where $\gcd(i, 15) = 1$; that is the $\phi(15) = 8$ elements

$\gamma = \alpha+1,\ \gamma^2 = \alpha^2+1,\ \gamma^4 = \alpha^3+\alpha^2+\alpha,\ \gamma^7 = \alpha^2+\alpha+1,\ \gamma^8 = \alpha^3+1,\ \gamma^{11} = \alpha^3+\alpha+1, \gamma^{13} = \alpha^2+\alpha, \gamma^{14} = \alpha^3+\alpha$

(c) Here, $\alpha^2 = -\alpha + 1 = 2\alpha + 1$.

i	0	1	2	3	4	5	6	7	8
α^i	1	α	$2\alpha + 1$	$2\alpha + 2$	2	2α	$\alpha + 2$	$\alpha + 1$	1

The element α is primitive, so all of the primitive elements of $\mathbb{Z}_3/\langle x^2 + x - 1\rangle$ are given by α^i where $\gcd(i, 8) = 1$; that is all of odd powers of α above:

$$\alpha\,, \quad \alpha^3 = 2\alpha + 2\,, \quad \alpha^5 = 2\alpha\,, \quad \alpha^7 = \alpha + 1$$

67. Here, we have that $\alpha^4 = \alpha + 1$.

$\alpha^0 = 1$	$\alpha^8 = \alpha^2 + 1$
$\alpha^1 = \alpha$	$\alpha^9 = \alpha^3 + \alpha$
$\alpha^2 = \alpha^2$	$\alpha^{10} = \alpha^2 + \alpha + 1$
$\alpha^3 = \alpha^3$	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
$\alpha^4 = \alpha + 1$	$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^5 = \alpha^2 + \alpha$	$\alpha^{13} = \alpha^3 + \alpha^2 + 1$
$\alpha^6 = \alpha^3 + \alpha^2$	$\alpha^{14} = \alpha^3 + 1$
$\alpha^7 = \alpha^3 + \alpha + 1$	$\alpha^{15} = 1$

Define $\beta = \alpha^3 + \alpha + 1$.

(a) By the table, we see that $\beta = \alpha^7$, so

$$(\alpha^3 + \alpha + 1)^{-1} = \beta^{-1} = \alpha^{-7} = \alpha^{15-7} = \alpha^8 = \alpha^2 + 1$$

(b) By the table,

$$\frac{(\alpha^3 + \alpha + 1)(\alpha + 1)}{\alpha^3 + 1} = \frac{\alpha^7 \alpha^4}{\alpha^{14}} = \alpha^{-3} = \alpha^{15-3} = \alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$$

(c) For $p = 2$, the powers $\beta^{p^i} = \alpha^{7\times 2^i}$ are

$$\alpha^7\,, \quad \alpha^{14}\,, \quad \alpha^{28} = \alpha^{13}\,, \quad \alpha^{56} = \alpha^{11}\,, \quad \alpha^{112} = \alpha^7\,,$$

so the minimal polynomial of $\beta = \alpha^3 + \alpha + 1 = \alpha^7$ is

$$\begin{aligned}
g(x) &= (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{13})(x - \alpha^{11}) \\
&= x^4 - (\alpha^7 + \alpha^{14} + \alpha^{13} + \alpha^{11})x^3 \\
&\quad + (\alpha^7\alpha^{14} + \alpha^7\alpha^{13} + \alpha^7\alpha^{11} + \alpha^{14}\alpha^{13} + \alpha^{14}\alpha^{11} + \alpha^{13}\alpha^{11})x^2 \\
&\quad - (\alpha^7\alpha^{14}\alpha^{13} + \alpha^7\alpha^{14}\alpha^{11} + \alpha^7\alpha^{13}\alpha^{11} + \alpha^{14}\alpha^{13}\alpha^{11})x \\
&\quad + \alpha^7\alpha^{14}\alpha^{13}\alpha^{11} \\
&= x^4 - (\alpha^7 + \alpha^{14} + \alpha^{13} + \alpha^{11})x^3 \\
&\quad + (\alpha^6 + \alpha^5 + \alpha^3 + \alpha^{12} + \alpha^{10} + \alpha^9)x^2 \\
&\quad - (\alpha^3 + \alpha^2 + \alpha + \alpha^8)x \\
&\quad + \alpha^0 \\
&= x^4 - ((\alpha^3 + \alpha + 1) + (\alpha^3 + 1) + (\alpha^3 + \alpha^2 + 1) + (\alpha^3 + \alpha^2 + \alpha)x^3 \\
&\quad + ((\alpha^3 + \alpha^2) + (\alpha^2 + \alpha) + \alpha^3 + (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^2 + \alpha + 1) + (\alpha^3 + \alpha))x^2 \\
&\quad - (\alpha^3 + \alpha^2 + \alpha + \alpha^2 + 1)x \\
&\quad + 1 \\
&= x^4 - x^3 - (\alpha^3 + \alpha + 1)x + 1 \\
&= x^4 + x^3 + 1
\end{aligned}$$

(d) The (primitive) elements $\alpha^1 = \alpha$, α^2, α^4, and α^8 have the (primitive) minimum polynomial $x^4 + x + 1$. The powers $(\alpha^3)^{2^i}$ are

$$\alpha^3\,, \quad \alpha^6\,, \quad \alpha^{12}\,, \quad \alpha^{24} = \alpha^9\,, \quad \alpha^{48} = \alpha^3\,,$$

so the minimal polynomial of α^3 is

$$\begin{aligned}
g(x) &= (x-\alpha^3)(x-\alpha^6)(x-\alpha^{12})(x-\alpha^9) \\
&= x^4 - (\alpha^3+\alpha^6+\alpha^{12}+\alpha^9)x^3 \\
&\quad + (\alpha^3\alpha^6+\alpha^3\alpha^{12}+\alpha^3\alpha^9+\alpha^6\alpha^{12}+\alpha^6\alpha^9+\alpha^{12}\alpha^9)x^2 \\
&\quad - (\alpha^3\alpha^6\alpha^{12}+\alpha^3\alpha^6\alpha^9+\alpha^3\alpha^{12}\alpha^9+\alpha^6\alpha^{12}\alpha^9)x \\
&\quad + \alpha^3\alpha^6\alpha^{12}\alpha^9 \\
&= x^4 - (\alpha^3+\alpha^6+\alpha^{12}+\alpha^9)x^3 \\
&\quad + (\alpha^9+\alpha^0+\alpha^{12}+\alpha^3+\alpha^0+\alpha^6)x^2 \\
&\quad - (\alpha^6+\alpha^3+\alpha^9+\alpha^{12})x \\
&\quad + \alpha^0 \\
&= x^4 - (\alpha^3+(\alpha^3+\alpha^2)+(\alpha^3+\alpha^2+\alpha+1)+(\alpha^3+\alpha))x^3 \\
&\quad + ((\alpha^3+\alpha)+1+(\alpha^3+\alpha^2+\alpha+1)+\alpha^3+1+(\alpha^3+\alpha^2))x^2 \\
&\quad - ((\alpha^3+\alpha^2)+\alpha^3+(\alpha^3+\alpha)+(\alpha^3+\alpha^2+\alpha+1))x \\
&\quad + 1 \\
&= x^4+x^3+x+1
\end{aligned}$$

The powers $(\alpha^5)^{2^i}$ are

$$\alpha^5\,, \quad \alpha^{10}\,, \quad \alpha^{20} = \alpha^5\,,$$

so the minimal polynomial of α^5 is

$$\begin{aligned}
g(x) &= (x-\alpha^5)(x-\alpha^{10}) \\
&= x^2 - (\alpha^5+\alpha^{10})x + \alpha^5\alpha^{10} \\
&= x^2 - ((\alpha^2+\alpha)+(\alpha^2+\alpha+1))x + \alpha^0 \\
&= x^2+x+1
\end{aligned}$$

The powers $(\alpha^5)^{2^i}$ are

$$\alpha^5\,, \quad \alpha^{10}\,, \quad \alpha^{20} = \alpha^5\,,$$

so the minimal polynomial of α^5 is

$$\begin{aligned}
g(x) &= (x-\alpha^5)(x-\alpha^{10}) \\
&= x^2 - (\alpha^5+\alpha^{10})x + \alpha^5\alpha^{10} \\
&= x^2 - ((\alpha^2+\alpha)+(\alpha^2+\alpha+1))x + \alpha^0 \\
&= x^2+x+1
\end{aligned}$$

We have thus found the minimal polynomials of the powers of α:

$$x^4+x^3+1\,, \quad x^4+x^3+x+1\,, \quad x^2+x+1$$