1. (i) As $x + 4$ has degree one, either it divides $x^3 - 6x + 7$ or these two polynomials are coprime. But if $x + 4$ divides $x^3 - 6x + 7$ then $x = -4$ is a root of $x^3 - 6x + 7$, which it obviously is not. Thus the gcd is 1.

(ii) We have $x^7 - x^4 = x^4(x^3 - 1)$. Hence

$$x^7 - x^4 + x^3 - 1 = x^4(x^3 - 1) + x^3 - 1 = (x^3 - 1)(x^4 + 1).$$

Thus the gcd is $x^3 - 1$.

2. We will repeatedly use the fact that if a polynomial of degree at most three is not irreducible, it must in fact have a root, as it must have a linear factor.

(i) $x^2 + 7$ cannot have a root over $\mathbb{R}$ as $a^2 + 7 \geq 7$, for all $a \in \mathbb{R}$.

(ii) This is slightly tricky. Probably the best way to proceed is as follows. Suppose that $a/b \in \mathbb{Q}$ is a root, where $a$ and $b$ are coprime integers. We have

$$(a/b)^3 - 3(a/b) + 3 = 0.$$

Multiplying through by $b^3$ gives,

$$a^3 - 3ab^2 + 3b^3 = 0.$$

Reducing modulo three, it follows that $a$ is divisible by 3. Thus $a = 3c$, some $c$. Substituting, we have

$$(3c)^3 - 3^2 cb^2 + 3b^3 = 0.$$

Cancelling one power of 3, we have

$$b^3 - 3b^2 c + 9c = 0.$$

Reducing modulo three again, we have that $b$ is divisible by three. But this contradicts the fact that $a$ and $b$ are chosen to be coprime.

(iii) It suffices to observe that $0 + 0 + 1 = 1 + 1 + 1 = 1 \neq 0$.

(iv) Note that we are asking if $-1$ is a square or not, in $\mathbb{F}_{19}$. As $(-a)^2 = a^2$, it suffices to consider $0 \leq a \leq 9$.

$$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 16 \quad 5^2 = 25 = 6, \quad 6^2 = 36 = -2, \quad 7^2 = 49 = 11, \quad 8^2 = 64 = 7, \quad 9^2 = 81 = 5.$$ 

Thus $x^2 + 1$ does not have a root and so it must be irreducible.
(v) Again it suffices to check that 9 is not a cube root in \( \mathbb{F}_{13} \). As \((-a)^3 = -a^3\), it suffices to check that for \(0 \leq a \leq 4\), \(a^3 \neq \pm 9 = 9, 4\). We compute
\[
0^3 = 0, \quad 1^3 = 1, \quad 2^3 = 8, \quad 3^3 = 27 = 1 \quad 4^3 = 64 = 12.
\]

(vi) We first check that \(x^4 + 2x^2 + 2\) does not have any linear factors. This is equivalent to checking that it does not have any roots, which is clear as
\[
a^4 + 2a^2 + 2 \geq 2
\]
for any real number \(a\).

The only other possibility to eliminate is that it is a product of quadratic factors. Suppose that
\[
x^4 + 2x^2 + 2 = f(x)g(x),
\]
where both \(f\) and \(g\) are quadratic. Moving the coefficient of \(x^2\) in \(f\) from \(f\) to \(g\), we might as well assume that \(f\) is monic, that is, that its top coefficient is 1. In this case \(g\) is monic as well. Thus
\[
x^4 + 2x^2 + 2 = (x^2 + ax + b)(x^2 + cx + d),
\]
where \(a, b, c\) and \(d\) are rational numbers. Comparing coefficients of \(x^3\), we get
\[
a + c = 0.
\]
Renaming, we get
\[
x^4 + 2x^2 + 2 = (x^2 + ax + b)(x^2 - ax + c).
\]
Looking the coefficient of \(x\), we get
\[
am - ab = 0.
\]
Thus either \(a = 0\) or \(b = c\). Suppose \(a = 0\). Replacing \(x^2\) by \(y\), we get
\[
y^2 + 2y + 2 = (y + a)(y + b),
\]
some \(a\) and \(b\). In this case the polynomial \(y^2 + 2y + 2\) would have a real root. But
\[
y^2 + 2y + 2 = (y + 1)^2 + 1
\]
so that if \(a \in \mathbb{R}\), we have
\[
a^2 + 2a + 2 = (a + 1)^2 + 1 \geq 1 > 0.
\]
The only remaining possibility is that \(b = c\). In this case \(b^2 = 2\), which is impossible, as \(b\) is a rational number.

3. We apply Euclid’s algorithm. As the norm of \(11 + 7i\) is greater than \(8 - i\), we first try to divide \(a = 8 - i\) into \(b = 11 + 7i\). Let \(c\) be the quotient in \(\mathbb{C}\). Now
\[
a\bar{a} = 64 + 1 = 65.
\]
Thus \( a^{-1} = \frac{1}{65} \bar{a} \). Hence

\[
c = \frac{b}{a} = a^{-1}b = \frac{1}{65}(\bar{b} a) = \frac{1}{65}(\bar{b} a) = \frac{1}{65}(b \bar{a}) = \frac{1}{65}(81 + 67i).
\]

Clearly the closest gridpoint \( q \) to \( c \) is \( 1 + i \). In this case

\[
r = b - qa = 11 + i - 9 - 7i = 4 - 6i.
\]

Thus

\[
11 + 7i = (1 + i)(8 - i) + (4 - 6i).
\]

We continue with \( 4 - 6i \) and \( 8 - i \). Thus we now try to divide \( 4 - 6i \) into \( 8 - i \). Note that

\[
(8 - i) - (4 - 6i) = 4 + 5i.
\]

It follows that we can take at the next step \( q = 1 \) and \( r = 4 + 5i \), as \( 4 + 5i \) has smaller norm than \( 4 - 6i \). Thus

\[
8 - i = 1(4 - 6i) + 4 + 5i.
\]

Now we try to divide \( 4 + 5i \) into \( 4 - 6i \). The inverse of \( 4 + 5i \) is

\[
\frac{1}{41}(4 - 5i).
\]

Thus we look for a gridpoint close to

\[
\frac{1}{41}(4 - 6i)(4 - 5i) = \frac{-1}{41}(14 + 44).
\]

Clearly we should take \(-i\). In this case the remainder is

\[
4 - 6i + i(4 + 5i) = -1 - 2i.
\]

We have

\[
4 - 6i = i(4 + 5i) - (1 + 2i).
\]
We continue with $1+2i$ and $4+5i$. In this case we can spot that $q = 2$, so that
\[ r = i. \]
As this is a unit, in fact the original numbers are coprime.

*Aliter:* Here is an entirely different way to proceed. Let $q = a + bi$ be a Gaussian prime. The norm of $q$ is $a^2 + b^2$. Moreover if $q$ divides $c + di$ then the norms must divide each other. Thus if $11 + 7i$ and $8 - i$ have any common factors, then their norms must have a common factor. The norm of the first number is $170 = 2 \cdot 5 \cdot 17$ and the norm of the second is $65 = 5 \cdot 13$. The only common factors are then 5. It follows that
\[ 11 + 7i = p_1p_2p_3, \]
where the norm of $p_1$ is 2, the norm of $p_2$ is 5 and the norm of $p_3$ is 17. Similarly
\[ 8 - i = q_1q_2, \]
where the norm of $q_1$ is 5 and the norm of $q_2$ is 13. Of course the $p$’s and the $q$’s are primes.

How does 5 factor in the Gaussian integers? Well
\[ 5 = 1^2 + 2^2 = (1 + 2i)(1 - 2i). \]
Moreover $1+2i$ and $1-2i$ are not associates. Thus, since the Gaussian integers are a UFD, the only possible common factors are $1 \pm 2i$, and if one divides $8 - i$ (or $11 + 7i$) then the other does not (as 5 divides the norm, but not $5^2$).

Now $8 - i$ is divisible by $1 - 2i$. Indeed
\[ 8 - i = (2 + 3i)(1 - 2i). \]
Thus $p_2 = 1 - 2i$. On the other hand, $11 + 7i$ is divisible by $1 + 2i$. Indeed
\[ 11 + 7i = (5 - 3i)(1 + 2i). \]
Thus $q_1 = 1 + 2i$. It follows that $11 + 7i$ and $8 - i$ are coprime.

4. Let
\[ \phi: \mathbb{R} \rightarrow \mathbb{C} \]
be the obvious inclusion. Applying the universal property of a polynomial ring, define a ring homomorphism
\[ \phi: \mathbb{R}[x] \rightarrow \mathbb{C} \]
by sending $x$ to $i$. $\phi$ is obviously surjective as $\mathbb{R} \cup \{i\}$ generates $\mathbb{C}$. Let $I$ be the kernel. This is an ideal in $\mathbb{R}[x]$. Therefore it must be principal. On the other hand $x^2 + 1$ is clearly in the kernel and $x^2 + 1$ is irreducible over $\mathbb{R}$, whence prime. It follows that $I = \langle x^2 + 1 \rangle$, and that $I$ is a prime ideal. By the Isomorphism Theorem, the result follows.
5. (i) To show that \(x^2 + 1\) is irreducible, it suffices to check that \(-1\) is not a square in \(F\). We compute \(a^2\), \(0 \leq a \leq 5\). We have

\[
0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 16 = 5, \quad 5^2 = 25 = 3.
\]

Thus \(x^2 + 1\) is irreducible. As \(F\) is a field, \(F[x]\) is a UFD. Thus \(x^2 + 1\) is prime. Thus \(I = \langle x^2 + 1 \rangle\) is a prime ideal and so

\[
L = F[x]/I,
\]

is an integral domain.

I claim that every element of \(L\) is represented uniquely by a polynomial of the form \(ax + b\), where \(a\) and \(b\) are in \(F\).

First suppose that we have a coset \(g + I\). By the division algorithm, we may write

\[
g = qf + r,
\]

where the degree of \(r\) is at most one and \(f = p\). Thus \(r = ax + b\), for some \(a\) and \(b\) and moreover \(g + I = r + I\).

On the other hand if \(ax + b + I = cx + d + I\), then \((a-c)x + (b-d) \in I\). On the other hand, as \(I\) is generated by a polynomial of degree two, the only non-zero elements of \(I\) have degree at least two. Thus \((a-c)x + b - d = 0\), so that \(a = c\) and \(b = d\). The claim follows.

In this case \(L\) has \(121 = 11^2\) elements. As \(L\) is finite, it is in fact a field and we are done.

(ii) It suffices, repeating the argument above, to show that \(x^3 + x + 4\) is irreducible. To prove this we show it does not have any roots. We compute

\[
\begin{align*}
0^3 + 0 + 4 & = 4 \\
1^3 + 1 + 4 & = 6 \\
2^3 + 2 + 4 & = 3 \\
3^3 + 3 + 4 & = 1 \\
4^3 + 4 + 4 & = 5 \\
5^3 + 5 + 4 & = 4 \\
6^3 + 6 + 4 & = -5^3 - 5 + 4 = 6 \\
7^3 + 7 + 4 & = -4^3 - 4 + 4 = 2 \\
8^3 + 8 + 4 & = -3^3 - 3 + 4 = 4 \\
9^3 + 9 + 4 & = -2^3 - 2 + 4 = 3 \\
10^3 + 10 + 4 & = -1^3 - 1 + 4 = 2.
\end{align*}
\]

6. Suppose that \(p_1, p_2, \ldots, p_n\) are irreducible polynomials. Then each \(p_i\) is not a constant polynomial, that is, its degree is at least one. Let

\[
f = p_1 \cdot p_2 \cdots p_n + 1.
\]

As \(R = F[x]\) is a UFD it follows that \(f\) is a product of primes, \(q_1, q_2, \ldots, q_m\). As \(p_1, p_2, \ldots, p_n\) are irreducible they are prime. Now \(p_i\) divides the first term on the RHS but not the second, so that \(p_i\) does not divide \(f\). Thus none of the primes \(q_1, q_2, \ldots, q_m\) are equal to \(p_1, p_2, \ldots, p_n\). Thus \(f\) is divisible by an irreducible polynomial, not equal to one of \(p_1, p_2, \ldots, p_n\).
It follows that there are infinitely many irreducible polynomials. Let $m$ be the cardinality of $F$. As there are $m^{d+1}$ polynomials of degree at most $d$, so that there are only finitely many polynomials of degree at most $d$, there must be polynomials of arbitrarily large degree.

7. Let $k$ be a field and let $S$ be the infinite polynomial ring

$$k[u, v, y, x_1, x_2, \ldots].$$

Let $I$ be the ideal generated by $x_1 y = uv$ and $x_i = x_{i+1}^2$, $i = 1, 2, \ldots$. Let $R$ be the ring $S/I$.

Consider $a = uv \in R$. Then $u$ and $v$ are clearly irreducible elements of $R$. On the other hand $a = x_1 y$, $x_1 = x_2^2$, $x_2 = x_3^2$ and so on, $x_1, x_2, \ldots$ are not units, so that $a$ is a product of irreducibles, whilst at the other time, one can run the factorisation algorithm, starting with $a$, so that it never terminates.

8. I am not sure how to do this without using some techniques from a little later in the course.