Exercise 2

(1) (a) Let $f(x) = c_n x^n + c_{n-1} x^{n-1} + c_{n-2} x^{n-2} + \cdots + c_1 x + c_0$

$$= (c_n x^n + c_n x^a - c_n x^a) + (c_{n-1} x^{n-1} + c_{n-1} a^{n-1} - c_{n-1} a^{n-1}) + \cdots$$

$$= (c_n x^n - c_n x^a) + (c_{n-1} x^{n-1} - c_{n-1} a^{n-1}) + \cdots + (c_1 x - c_1 a)$$
$$+ (c_n a^n + c_{n-1} a^{n-1} + \cdots + c_1 a)$$

$$= (x-a)(c_n x^{n-1} - c_n a^{n-1} + \cdots + c_1 - c_1) + f(a)$$

$$= (x-a)\, q(x) + \underbrace{f(a)}_{\text{remainder}} \quad \text{for some } q(x) \in \mathbb{K}[x].$$

(b) According to part (a), $f(x) \equiv f(a) \bmod (x-a)$.
Therefore, $(x-a) \mid f(x) \Leftrightarrow f(x) \equiv 0 \bmod (x-a) \Leftrightarrow f(a) = 0$.

(c) From part (a) we've seen that the highest degree of $q(x)$ is $n-1$. Since we know that a degree-one polynomial has at most one root, by induction, $f(x)$ has at most n roots, since it can be "reduced" to a degree-one polynomial in $n-1$ steps of doing $f(x) = (x-a)q(x) + f(a)$.

(2) Given any polynomial $f(x) \in \mathbb{F}_p[x]$ where $f(x) = c_n x^n + \cdots + c_1 x + c_0$, Try dividing $f(x)$ by $g(x) = d_n x^n + \cdots + d_1 x + d_0$, where $d_i \in \{0, \dots, p-1\}$ for $0 \le i < n$. If $g(x) \mid f(x)$ then $g(x)$ is a factor of $f(x)$. Since there are finitely many possible $g(x)$'s to try, the algorithm will eventually terminate.

(3) x^4+1

(4) $\mathbb{F}_3[x]/(x^4+1)$ is a field with 81 elements where representatives have the form $c_3x^3+c_2x^2+c_1x+c_0$ and $c_i \in \{0,1,2\}$.

Exercise 3

(1) Times table for $\mathbb{F}_3[x]/(x^2+1)$:

1	2	x	x+1	x+2	2x	2x+1	2x+2
2	1	2x	2x+2	2x+1	x	x+2	x+1
x	2x	2	x+2	2x+2	1	x+1	2x+1
x+1	2x+2	x+2	2x	1	2x+1	2	x
x+2	2x+1	2x+2	1	x	x+1	2x	2
2x	x	1	2x+1	x+1	2	2x+2	x+2
2x+1	x+2	x+1	2	2x	2x+2	x	1
2x+2	x+1	2x+1	x	2	x+2	1	2x

Times table for $\mathbb{Z}[i]/(3)$ is basically ⇧ with every x replaced by i.

(2) Let $x = a_1 + b_1\sqrt{D},\ y = a_2 + b_2\sqrt{D}$. Then,

$$N(xy) = N(\ (a_1+b_1\sqrt{D})(a_2+b_2\sqrt{D})\ ) = N(\ a_1a_2 + a_1b_2\sqrt{D} + a_2b_1\sqrt{D} + b_1b_2D\ )$$

$$= N(\ (a_1a_2+b_1b_2D) + (a_1b_2+a_2b_1)\sqrt{D}\ ) = (a_1a_2+b_1b_2D)^2 - (a_1b_2+a_2b_1)^2 D$$

$$= a_1^2a_2^2 + 2a_1a_2b_1b_2D + b_1^2b_2^2D^2 - a_1^2b_2^2D\ 2a_1a_2b_1b_2D - a_2^2b_1^2D$$

$$= a_1^2a_2^2 - a_1^2b_2^2D - a_2^2b_1^2D + b_1^2b_2^2D^2$$

$$= (a_1^2 - b_1^2D)(a_2^2 - b_2^2D) = N(a_1+b_1\sqrt{D})N(a_2+b_2\sqrt{D}) = N(x)N(y)$$

(3) If it exists, the mult. inverse of $2+5i = \frac{1}{2+5i}$.

$$\frac{1}{2+5i} = \frac{2-5i}{(2+5i)(2-5i)} = \frac{2-5i}{29} = \frac{2}{29} - \frac{5}{29}i$$

$$\left.\begin{array}{l} x = \frac{2}{29} \Rightarrow 29x \equiv 2 \bmod 31 \Rightarrow x \equiv 30 \bmod 31 \\ x = -\frac{5}{29} \Rightarrow 29x \equiv -5 \bmod 31 \Rightarrow x \equiv 18 \bmod 31 \end{array}\right\} \boxed{30+18i}$$

Meanwhile, $2+5i$ cannot have a multiplicative inverse in $\mathbb{Z}[i]/(29)$ since its "potential" inverse $\frac{2-5i}{29}$ has $29 \equiv 0 \bmod 29$ in denom.

(4) $$\frac{1}{7-3\sqrt{5}} = \frac{7+3\sqrt{5}}{49-45} = \frac{7}{4} + \frac{3}{4}\sqrt{5}$$

in mod 11, $\left\{\begin{array}{l} 7/4 \equiv 10 \bmod 11 \\ 3/4 \equiv 9 \bmod 11 \end{array}\right\} \boxed{10+9\sqrt{5}}$

in mod 17, $\left\{\begin{array}{l} 7/4 \equiv 6 \bmod 11 \\ 3/4 \equiv 5 \bmod 11 \end{array}\right\} \boxed{6+5\sqrt{5}}$

(5) We know that $\varphi = \frac{1+\sqrt{5}}{2}$ is the root of $x^2 - x - 1 = 0$ which is in the form of $x^2 + ax + b$ (for $a = b = -1$). Therefore, $\boxed{\text{yes}}$.

(6) Since we know that $a + b\sqrt{5}$ is a quadratic integer when it is the root of $x^2 - 2ax + (a^2 - b^2 \cdot 5)$. Therefore, $a + b\sqrt{5}$ is quadratic integer when $a, b \in \mathbb{Z}$.