20.4

Note that

$$3^{47} = 3^{2\cdot 22+3} = \left(3^{23-1}\right)^2 \cdot 3^3.$$

By Fermat's Little Theorem, $3^{23-1} \equiv 1 \pmod{23}$ and therefore $\left(3^{23-1}\right)^2 \equiv 1 \pmod{23}$. Since $3^3 = 27 \equiv 4 \pmod{23}$ it follows

$$3^{47} \equiv 1 \cdot 4 \equiv 4 \pmod{23}.$$

20.6

First note that

$$2^{17} \equiv \left(2^4\right)^4 \cdot 2 \equiv (-2)^4 \cdot 2 \equiv 16 \cdot 2 \equiv 14 \pmod{18}.$$

Therefore $2^17 = 18m + 14$ for some $m \in \mathbb{Z}$. Hence

$$2^{2^{17}} = 2^{18m+14} = \left(2^{18}\right)^m \cdot 2^{14} = \left(2^{19-1}\right)^m \cdot 2^{14}.$$

Since 19 is prime, then

$$2^{18} \equiv 2^{19-1} \equiv 1 \pmod{19}$$

meaning

$$2^{2^{17}} \equiv \left(2^{19-1}\right)^m \cdot 2^{14} \equiv 1^m \cdot 2^{14} \equiv 2^{14} \equiv \left(2^7\right)^2 \equiv (-5)^2 \equiv 6 \pmod{19}$$

which adding one gives the final result $7 \pmod{19}$.

20.12

The congruence relation reduces to

$$7x \equiv 5 \pmod{15}.$$

Since $\gcd(7, 15) = 1$ which divides 5, there exists solutions. Since $7 \cdot 5 = 5 \pmod{15}$ the solutions are

$$x = 5m + 15, m \in \mathbb{Z}.$$

20.14

The congruence relation reduces to

$$21x \equiv 15 \pmod{24}.$$

Since $\gcd(21, 24) = 3$ which divides 15, there exists solutions. Consider the congruence relation

$$7x \equiv 5 \pmod{8}.$$

This has a solution $x = 3$ meaning the solutions to the original are the elements of $3 + 8\mathbb{Z}$.

20.27

Proof. Let $a \in \mathbb{Z}_p$. Then $a^2 - 1 = (a-1)(a+1) = 0$. Since $\mathbb{Z}_p$ is a field, it has no zero divisors meaning $a-1$ or $a+1$ are zero and hence $a = 1$ or $a = p-1$. ■

20.28

Proof. Note that

$$(p-1)! = (p-1)(p-2)(p-3)\cdots(3)(2)(1).$$

For $p \geq 3$, the elements exclusively between $p-1$ and 1 will have their multiplicative inverse in this factorial expansion meaning

$$(p-1)! = (p-1)(1)\cdots(1)(1) = p-1 \equiv -1 \pmod{p}.$$

In the case that $p = 2$, $(p-1)! = (2-1)! = 1 \equiv -1 \pmod 2$ and for $p = 1$, $(p-1)! = 0! = 1 \equiv -1 \pmod 1$. ■

20.29

Consider each prime factor individually. Note that only the cases where n isnt divisible by a prime factor need to be considerd since otherwise if n is divisible by all prime factors, $n^{37} - n = n(n^{36} - 1)$ is as well.

37) Since $n^{37} \equiv n \pmod{37}$ it follows $n^{37} - n = 0 \equiv \pmod{37}$ so 37 dividies

19) Assume that 19 doesn't divide n. Then $n^{36} - 1 \equiv \left(n^{18}\right)^2 - 1 \equiv 1^2 - 1 \equiv 0 \pmod{19}$ therefore 19 divides

13 Assume 13 doesnt divide n. Then $n^{36} - 1 \equiv \left(n^{12}\right)^3 - 1 \equiv 1^3 - 1 \equiv 0 \pmod{13}$ therefore 13 divides

7) Assume 7 doesnt divide n. Then $n^{36} - 1 \equiv \left(n^6\right)^6 - 1 \equiv 1^6 - 1 \equiv 0 \pmod 7$ therefore 7 divides

3) Assume 3 doesnt divide n. Then $n^{36} - 1 \equiv \left(n^2\right)^{18} - 1 \equiv 1^{18} - 1 \equiv 0 \pmod 3$ therefore 3 divides

2) Assume 2 doesnt divide n. Then $n^{36} - 1 \equiv \left(n^1\right)^{36} - 1 \equiv 1^{36} - 1 \equiv 0 \pmod 2$ therefore 2 divides

21.2

The field of quotients for D are $\left\{q + p\sqrt{2} : p, q \in \mathbb{Q}\right\}$ since the multiplicative inverse of an element in D would look like

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

of which $\frac{a}{a^2-2b^2}$ and $\frac{-b}{a^2-2b^2}$ are rational numbers.

21.6

Proof. Let $[(a_1, b_1)]$, $[(a_2, b_2)]$ and $[(a_3, b_3)]$ be elements of F. Then

$$\begin{aligned}\Big([(a_1, b_1)] + [(a_2, b_2)]\Big) + [(a_3, b_3)] &= [(a_1b_2 + a_2b_1, b_1b_2)] + [(a_3, b_3)] \\ &= [(a_1b_2b_3 + a_2b_1b_3 + a_3b_1b_2, b_1b_2b_3)]\end{aligned}$$

and

$$\begin{aligned}[(a_1, b_1)] + \Big([(a_2, b_2)] + [(a_3, b_3)]\Big) &= [(a_1, b_1)] + [(a_2b_3 + a_3b_2, b_2b_3)] \\ &= [(a_1b_1b_2 + a_2b_1b_3 + a_3b_1b_2, b_3b_2b_1)].\end{aligned}$$

Since addition and multiplication for D is associative and abelian, these can be rearranged to equal each other and hence addition on F is associative. ■

21.7

Proof. Let $[(a, b)] \in F$. Then

$$[(0, 1)] + [(a, b)] = [(0b + 1a, 1b)] = [(a, b)].$$

Since addition on F is commutative, it follows $[(0, 1)]$ is an additive identity in F. ■

21.8

Proof. Let $[(a, b)] \in F$. Note that

$$[(a, b)] + [(-a, b)] = [(ab + b(-a), b^2)] = [(ab - ab, b^2)] = [(0, b^2)] = [(0, 1)].$$

Since addition is commutative, it follows $[(-a, b)]$ is the additive inverse for any element in F. ■

21.9

Proof. Let $[(a_1, b_1)]$, $[(a_2, b_2)]$ and $[(a_3, b_3)]$ be elements of F. Then

$$\Big([(a_1, b_1)][(a_2, b_2)]\Big)[(a_3, b_3)] = [(a_1a_2, b_1b_2)][(a_3, b_3)] = [(a_1a_2a_3, b_1b_2b_3)]$$

and

$$[(a_1, b_1)]\Big([(a_2, b_2)][(a_3, b_3)]\Big) = [(a_1, b_1)][(a_2a_3, b_2b_3)] = [(a_1a_2a_3, b_1b_2b_3)]$$

which are equal. Therefore multiplication on F is associative. ■

21.10

Proof. Let $[(a_1, b_1)], [(a_2, b_2)] \in F$. Then

$$[(a_1, b_1)][(a_2, b_2)] = [(a_1a_2, b_1b_2)] = [(a_2a_1, b_2b_1)] = [(a_2, b_2)][(a_1, b_1)]$$

since multiplication on D is commutative. Therefore multiplication on F is commutative. ■

21.11

Proof. Let $[(a_1, b_1)], [(a_2, b_2)]$ and $[(a_3, b_3)]$ be elements of F. Then

$$\begin{aligned}[(a_1, b_1)]\Big([(a_2, b_2)] + [(a_3, b_3)]\Big) &= [(a_1, b_1)][(a_2b_3 + a_3b_2, b_2b_3)] \\ &= [(a_1a_2b_3 + a_1b_3b_2, b_1b_2b_3)]\end{aligned}$$

and

$$\begin{aligned}[(a_1, b_1)][(a_2, b_2)] + [(a_1, b_1)][(a_3, b_3)] &= [(a_1a_2, b_1b_2)] + [(a_1a_3, b_1b_3)] \\ &= [(a_1a_2b_1b_3 + a_1a_3b_1b_2, b_1^2b_2b_3)]\end{aligned}$$

which are equal since by the definition of the equivalence for F

$$[(a_1a_2b_1b_3 + a_1a_3b_1b_2, b_1^2b_2b_3)] = [(a_1a_2b_3 + a_1a_3b_2, b_1b_2b_3)].$$

Since multiplication is commutative on F, the right distributive law also holds. Hence both laws hold on F. ■