VE203
Assignment 3

Jiang Yicheng
515370910224

October 7, 2016

1 Roots of Unity

1.1

$\forall a, b \in S, |a \cdot b| = |a| \cdot |b| = 1 \cdot 1 = 1$, so $a \cdot b \in S$.

$\forall a, b, c \in S$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ holds because of the property of multiplication of complex numbers. So the associativity holds.

Since $|1| = 1$ and $1 \in \mathbb{C}$, $1 \in S$. Moreover, $\forall a \in S$, $a \cdot 1 = 1 \cdot a = a$, so 1 is a unit element.

$\forall a \in S, |a| = 1 \neq 0$, so $1 = \dfrac{1}{|a|} = \left|\dfrac{1}{a}\right|$, and therefore $\dfrac{1}{a} \in S$. Since $\forall a \in S, a \cdot \dfrac{1}{a} = \dfrac{1}{a} \cdot a = 1$ and 1 is a unit element, then for any element in S, its inverse exists in S.

To sum up, $(S, \cdot)$ is a group.

1.2

$\forall a, b \in S(n), (a \cdot b)^n = a^n \cdot b^n = 1 \cdot 1 = 1$, so $a \cdot b \in S$.

$\forall a, b, c \in S(n)$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ holds because of the property of multiplication of complex numbers. So the associativity holds.

Since $1^n = 1$ and $1 \in \mathbb{C}$, $1 \in S(n)$. Moreover, $\forall a \in S$, $a \cdot 1 = 1 \cdot a = a$, so 1 is a unit element.

$\forall a \in S(n), a^n = 1 \neq 0$, so $1 = \dfrac{1}{a^n} = \left(\dfrac{1}{a}\right)^n$, and therefore $\dfrac{1}{a} \in S(n)$. Since $\forall a \in S, a \cdot \dfrac{1}{a} = \dfrac{1}{a} \cdot a = 1$ and 1 is a unit element, then for any element in $S(n)$, its inverse exists in $S(n)$.

To sum up, $(S(n), \cdot)$ is a group.

2 Matrix Groups

2.1

$$\forall A(\varphi_1) = \begin{pmatrix} cos(\varphi_1) & -sin(\varphi_1) \\ sin(\varphi_1) & cos(\varphi_1) \end{pmatrix}, A(\varphi_2) = \begin{pmatrix} cos(\varphi_2) & -sin(\varphi_2) \\ sin(\varphi_2) & cos(\varphi_2) \end{pmatrix} \in S,$$

$$A(\varphi_1) \cdot A(\varphi_2) = \begin{pmatrix} cos(\varphi_1) & -sin(\varphi_1) \\ sin(\varphi_1) & cos(\varphi_1) \end{pmatrix} \cdot \begin{pmatrix} cos(\varphi_2) & -sin(\varphi_2) \\ sin(\varphi_2) & cos(\varphi_2) \end{pmatrix} = \begin{pmatrix} cos(\varphi_1 + \varphi_2) & -sin(\varphi_1 + \varphi_2) \\ sin(\varphi_1 + \varphi_2) & cos(\varphi_1 + \varphi_2) \end{pmatrix}$$

so $A(\varphi_1) \cdot A(\varphi_2) \in S$.

$\forall A(\varphi_1), A(\varphi_2), A(\varphi_3) \in S, A(\varphi_1) \cdot (A(\varphi_2) \cdot A(\varphi_3)) = (A(\varphi_1) \cdot A(\varphi_2)) \cdot A(\varphi_3)$ holds because of the property of matrix multiplication. So the associativity holds.

Since $A(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in S$, and $\forall A(\varphi) \in S$, $A(0) \cdot A(\varphi) = A(\varphi) \cdot A(0) = A(\varphi)$, so $A(0)$ is a unit element.

$\forall \varphi \in \mathbb{R}, A(\varphi) \in S$, $A(-\varphi) \in S$. Since

$$\begin{aligned} A(\varphi) \cdot A(-\varphi) &= \begin{pmatrix} cos(\varphi + (-\varphi)) & -sin(\varphi + (-\varphi)) \\ sin(\varphi + (-\varphi)) & cos(\varphi + (-\varphi)) \end{pmatrix} \\ &= \begin{pmatrix} cos(0) & -sin(0) \\ sin(0) & cos(0) \end{pmatrix} \\ &= A(0) \end{aligned}$$

which is a unit element, then for any element in S, its inverse exists in S.

To sum up, $(S, \cdot)$ is a group.

2.2

a) $\forall A, B \in SL(n,\mathbb{R}), det(A \cdot B) = det(A) \cdot det(B) = 1 \cdot 1 = 1$ so $A \cdot B \in SL(n,\mathbb{R})$.

$\forall A, B, C \in SL(n,\mathbb{R})$, $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ holds because of the property of matrix multiplication. So the associativity holds.

Since $\det(\mathbb{1}) = 1$ where $\mathbb{1}$ is the unit matrix and $\mathbb{1} \in Mat(n \times n, \mathbb{R})$, $\mathbb{1} \in SL(n,\mathbb{R})$. And we know that $\forall A \in SL(n,\mathbb{R}), A \cdot \mathbb{1} = \mathbb{1} \cdot A = A$, so $\mathbb{1}$ is a unit element.

$\forall A \in SL(n,\mathbb{R})$, $det(A) = 1$, so A is invertible, i.e. $\exists A^{-1}$ such that $A \cdot A^{-1} = A^{-1} \cdot A = \mathbb{1}$. Then $det(A) \cdot det(A^{-1}) = det(A \cdot A^{-1}) = det(\mathbb{1}) = 1$. So $det(A^{-1}) = \dfrac{1}{det(A)} = 1$. So $A^{-1} \in SL(n,\mathbb{R})$.

To sum up, $(SL(n,\mathbb{R}), \cdot)$ is a group.

b) $\forall A, B \in SL(n,\mathbb{R})$,

$$\begin{aligned}(A \cdot B) \cdot (A \cdot B)^T =& (A \cdot B) \cdot (B^T \cdot A^T)) = A \cdot (B \cdot B^{-1}) \cdot A^{-1} \\ =& A \cdot \mathbb{1} \cdot A^{-1} = A \cdot A^{-1} \\ =& \mathbb{1}\end{aligned}$$

so $(A \cdot B)^{-1} = (A \cdot B)^T$. So $A \cdot B \in SL(n,\mathbb{R})$.

$\forall A, B, C \in O(n,\mathbb{R})$, $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ holds because of the property of matrix multiplication. So the associativity holds.

Since $(\mathbb{1})^T = \mathbb{1} = (\mathbb{1})^{-1}$ where $\mathbb{1}$ is the unit matrix, $\mathbb{1} \in O(n,\mathbb{R})$. And we know that $\forall A \in O(n,\mathbb{R}), A \cdot \mathbb{1} = \mathbb{1} \cdot A = A$, so $\mathbb{1}$ is a unit element.

$\forall A \in O(n,\mathbb{R})$, A is invertible, i.e. $\exists A^{-1}$ such that $A \cdot A^{-1} = A^{-1} \cdot A = \mathbb{1}$. Then

$$A \cdot A^{-1} = \mathbb{1} \Rightarrow (A^{-1})^T \cdot A^T = (A \cdot A^{-1})^T = (\mathbb{1})^T = \mathbb{1} \Rightarrow (A^{-1})^T = (A^T)^{-1}$$

Since $A^T = A^{-1}$, $(A^{-1})^T = (A^T)^{-1} = (A^{-1})^{-1}$. So $A^{-1} \in O(n,\mathbb{R})$.

To sum up, $(O(n,\mathbb{R}), \cdot)$ is a group.

c) From **a)b)** we can prove that $\forall A, B \in SO(n,\mathbb{R})$, $A \cdot B \in SO(n,\mathbb{R})$.

$\forall A, B, C \in SO(n,\mathbb{R})$, $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ holds because of the property of matrix multiplication. So the associativity holds.

Since $\det(\mathbb{1}) = 1, (\mathbb{1})^T = \mathbb{1} = (\mathbb{1})^{-1}$ where $\mathbb{1}$ is the unit matrix, $\mathbb{1} \in SO(n,\mathbb{R})$. And we know that $\forall A \in SO(n,\mathbb{R}), A \cdot \mathbb{1} = \mathbb{1} \cdot A = A$, so $\mathbb{1}$ is a unit element.

$\forall A \in SO(n,\mathbb{R})$, from **a)b)**, we can prove that $\exists A^{-1} \in Mat(n \times n, \mathbb{R}), A \cdot A^{-1} = \mathbb{1}, det(A^{-1}) = 1$ and $(A^{-1})^T = (A^{-1})^{-1}$. So $A^{-1} \in SO(n,\mathbb{R})$.

To sum up, $(SO(n,\mathbb{R}), \cdot)$ is a group.

3

3.1

1. $\forall m \in \mathbb{Z}, (m, m) \in R$ since $2\big|0$,i.e.$2|(m - m)$, which shows that the relation is reflexive.
2. $\forall (m, n) \in R, 2|(n - m)$. So $2|(m - n)$. So $(n, m) \in R$. So the relation is symmetric.
3. $\forall (m, n), (n, p) \in R, 2|(n - m), 2|(p - n)$. So $2|((n - m) + (p - n))$, i.e. $2|(p - m)$. So $(m, p) \in R$. So the relation is transitivity.

To sum up, $\sim$ is an equivalence relation.

3.2

Denote $2\mathbb{Z}$ as the set of all even number, and $2\mathbb{Z}+1$ as the set of all odd number. Then

$$2\mathbb{Z} \cap 2\mathbb{Z}+1 = \varnothing, \qquad 2\mathbb{Z} \cup 2\mathbb{Z}+1 = \mathbb{Z}$$

so $\{2\mathbb{Z}, 2\mathbb{Z}+1\}$ is a partition of a set $\mathbb{Z}$. We can see that this is induced by $\sim$ since $\forall a, b \in 2\mathbb{Z}$ or $2\mathbb{Z}+1$,$2|(b-a)$, so $a \sim b$; while $\forall a \in 2\mathbb{Z}, b \in 2\mathbb{Z}+1$, $b-a, a-b$ is not even number. So

$$a \in [b] \Leftrightarrow a \sim b \Leftrightarrow a, b \in 2\mathbb{Z} \ or \ 2\mathbb{Z}+1$$

To sum up, the partition induced by $\sim$ is $\{2\mathbb{Z}, 2\mathbb{Z}+1\}$.

3.3

From 3.2 we know that $2\mathbb{Z} = [a]$ if a is even and $2\mathbb{Z}+1 = [a]$ if a is odd.

1. $\forall m, n \in 2\mathbb{Z}$, $m+n, m \cdot n \in 2\mathbb{Z}$, so $[m+n] = 2\mathbb{Z}, [m \cdot n] = 2\mathbb{Z}$
2. $\forall m, n \in 2\mathbb{Z}+1$, $m+n \in 2\mathbb{Z}, m \cdot n \in 2\mathbb{Z}+1$, so $[m+n] = 2\mathbb{Z}, [m \cdot n] = 2\mathbb{Z}+1$
3. $\forall m \in 2\mathbb{Z}, n \in 2\mathbb{Z}+1$, $m+n \in 2\mathbb{Z}+1, m \cdot n \in 2\mathbb{Z}$, so $[m+n] = 2\mathbb{Z}+1, [m \cdot n] = 2\mathbb{Z}$
4. $\forall m \in 2\mathbb{Z}+1, n \in 2\mathbb{Z}$, $m+n \in 2\mathbb{Z}+1, m \cdot n \in 2\mathbb{Z}$, so $[m+n] = 2\mathbb{Z}+1, [m \cdot n] = 2\mathbb{Z}$

So we can see that these operations are independent of the representatives m and n of each class.

3.4

$\forall [a], [b] \in \mathbb{Z}_2$, since $a+b \in \mathbb{Z}$, $[a]+[b] = [a+b] \in \mathbb{Z}_2$.

$\forall [a], [b], [c] \in \mathbb{Z}_2$, $[a]+([b]+[c]) = [a]+[b+c] = [a+(b+c)] = [(a+b)+c] = [a+b]+[c] = ([a]+[b])+[c]$. So the associativity holds.

$\forall [a], [b] \in \mathbb{Z}_2$, $[a]+[b] = [a+b] = [b+a] = [b]+[a]$. So commutativity holds.

Since $[0] \in \mathbb{Z}_2$ and $\forall [a] \in \mathbb{Z}_2, [a]+[0] = [0]+[a] = [0+a] = [a]$, so $[0]$ is a unit element.

$\forall a \in \mathbb{Z}, [a], [-a] \in \mathbb{Z}_2$, and $[a]+[-a] = [-a]+[a] = [-a+a] = [0]$ which is a unit element, so for any element in $\mathbb{Z}_2$, its inverse exists in $\mathbb{Z}_2$.

So $(\mathbb{Z}_2, +)$ is an abelian group.

$\forall [a], [b] \in \mathbb{Z}_2$, since $a \cdot b \in \mathbb{Z}$, $[a] \cdot [b] = [a \cdot b] \in \mathbb{Z}_2$.

$\forall [a], [b], [c] \in \mathbb{Z}_2$, $[a] \cdot ([b] \cdot [c]) = [a] \cdot [b \cdot c] = [a \cdot (b \cdot c)] = [(a \cdot b) \cdot c] = [a \cdot b] \cdot [c] = ([a] \cdot [b]) \cdot [c]$. So the associativity holds.

$\forall [a], [b] \in \mathbb{Z}_2$, $[a] \cdot [b] = [a \cdot b] = [b \cdot a] = [b] \cdot [a]$. So commutativity holds.

Since $[1] \in \mathbb{Z}_2$ and $\forall [a] \in \mathbb{Z}_2, [a] \cdot [1] = [1] \cdot [a] = [1 \cdot a] = [a]$, so $[1]$ is a unit element.

$\forall [a], [b], [c] \in \mathbb{Z}_2, [a] \cdot ([b]+[c]) = [a] \cdot [b+c] = [a \cdot (b+c)] = [a \cdot b + a \cdot c] = [a \cdot b] + [a \cdot c] = [a] \cdot [b] + [a] \cdot [c]$, and $([b]+[c]) \cdot [a] = [a] \cdot ([b]+[c]) = [a \cdot b] + [a \cdot c] = [b \cdot a] + [c \cdot a] = [b] \cdot [a] + [c] \cdot [a]$. So distributivity holds.

So $(\mathbb{Z}_2, +, \cdot)$ is a commutative ring.

Since $[0]$ is unit element of addition and $[1]$ is unit element of multiplication, $[0] = 2\mathbb{Z}, [1] = 2\mathbb{Z}+1$, then $[0] \neq [1]$.

$\forall [a] \in \mathbb{Z}_2 \backslash \{[0]\}$, $a \neq 0$, so $\dfrac{1}{a} \in \mathbb{Z}$, and $[a] \cdot [\dfrac{1}{a}] = [a \cdot \dfrac{1}{a}] = [1]$

To sum up, $(\mathbb{Z}_2, +, \cdot)$ is a field.

4

Since $a, b \in \mathbb{Z}$, and $|a| + |b| \neq 0$, according to Bezout's Lemma, $\exists x_0, y_0 \in \mathbb{Z}$ such that

$$gcd(a, b) = ax_0 + by_0$$

$\forall k \in \mathbb{Z}$, $k \cdot gcd(a, b) = k \cdot (ax_0 + by_0) = a(kx_0) + b(ky_0)$, since $kx_0, ky_0 \in \mathbb{Z}$, $k \cdot gcd(a, b) \in T(a, b)$. So all integer multiples of $gcd(a, b)$ are in $T(a, b)$.

On the other hand, set $d = gcd(a, b)$, $\forall n \in T(a, b), \exists x, y \in \mathbb{Z}$, such that $n = ax + by$. Since $d|a$ and $d|b$, $d|(ax + by)$. So there exists some integer k such that $n = ax + by = k \cdot d$. So n is in the set of all integer multiples of $gcd(a, b)$.

To sum up, $T(a, b) = \{n \in \mathbb{Z} : n = ax + by, x, y \in \mathbb{Z}\}$ is the set of all integer multiples of $gcd(a, b)$.

5

$\forall n \in \mathbb{N}$, according to Division Algorithm, there exists unique $q, r \in \mathbb{Z}$ such that

$$n = 3q + r, \qquad r = 0, 1, 2$$

1. If $n = 3q + 0$, then $n^2 = 9q^2 = 3 \cdot 3q^2$. Since $q \in \mathbb{Z}$, $3q^2 \in \mathbb{N}$. So $\exists k \in \mathbb{N}$ such that $n^2 = 3k$.
2. If $n = 3q + 1$, then $n^2 = 9q^2 + 6q + 1 = 3 \cdot (3q^2 + 2q) + 1$. Since $n^2 \in \mathbb{N}, q \in \mathbb{Z}$, $3q^2 + 2q \in \mathbb{Z}$. If $3q^2 + 2q < 0$, then $3q^2 + 2q \leqslant -1$ and $n^2 = 3 \cdot (3q^2 + 2q) + 1 \leqslant -2 < 0$ which is contradiction. So $3q^2 + 2q \in \mathbb{N}$. So $\exists k \in \mathbb{N}$ such that $n^2 = 3k + 1$.
3. If $n = 3q+2$, then $n^2 = 9q^2+12q+4 = 3\cdot(3q^2+4q+1)+1$. Since $n^2 \in \mathbb{N}, q \in \mathbb{Z}$, $3q^2+2q \in \mathbb{Z}$. If $3q^2 + 4q + 1 < 0$, then $3q^2 + 4q + 1 \leqslant -1$ and $n^2 = 3 \cdot (3q^2 + 4q + 1) + 1 \leqslant -2 < 0$ which is contradiction. So $3q^2 + 4q + 1 \in \mathbb{N}$.So $\exists k \in \mathbb{N}$ such that $n^2 = 3k + 1$.

To sum up, for any $n \in \mathbb{N}$ there exists a $k \in \mathbb{N}$ such that either $n^2 = 3k$ or $n^2 = 3k + 1$.

6

According to Lemma 1.6.20, since $a + n, a, 1, n \in \mathbb{Z}$ and $a + n = a \cdot 1 + n$, then

$$gcd(a + n, a) = gcd(a, n)$$

Since $gcd(a, n)|n$, $gcd(a + n, a)|n$. Then $gcd(a + 1, a)|1$ for $n = 1$. So $gcd(a + 1, a) = \pm 1$. Since $gcd(a + 1, a) > 0$, $gcd(a + 1, a) = 1$. So a and $a + 1$ are relatively prime.

To sum up, $gcd(a, a + n)$ divides n, and a and $a + 1$ are always relatively prime.

7

7.1 56x+72y=40

$$56x + 72y = 40 \Leftrightarrow 7x + 9y = 5$$

$$9 = 1 \cdot 7 + 2$$
$$7 = 3 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

So according to The Euclidean Algorithm, $gcd(7,9)=1$. And $20\cdot 7-15\cdot 9=5$, so $x=20, y=-15$ is a solution. So all the solutions are

$$x=20+\frac{9}{1}t=20+9t, y=-15-\frac{7}{1}t=-15-7t, t\in\mathbb{Z}$$

To sum up, all $x,y\in\mathbb{Z}$ such that $56x+72y=40$ are

$$x=20+9t, y=-15-7t, t\in\mathbb{Z}$$

7.2 84x-439y=156

$$\begin{aligned}-439&=-6\cdot 84+65\\ 84&=1\cdot 65+19\\ 65&=3\cdot 19+8\\ 19&=2\cdot 8+3\\ 8&=2\cdot 3+2\\ 3&=1\cdot 2+1\\ 2&=2\cdot 1+0\end{aligned}$$

So according to The Euclidean Algorithm, $gcd(84,-439)=1$. And $84\cdot(-25272)-439\cdot(-4836)=156$, so $x=-25272, y=-4836$ is a solution. So all the solutions are

$$x=-25272+\frac{-439}{1}t=-25272-439t, y=-4836-\frac{84}{1}t=-4836-84t, t\in\mathbb{Z}$$

To sum up, all $x,y\in\mathbb{Z}$ such that $84x-439y=156$ are

$$x=-25272-439t, y=-4836-84t, t\in\mathbb{Z}$$

8

8.1

Since $a,b\in\mathbb{N}\backslash\{0\}$, then according to Bezout's Lemma, $\exists x_0,y_0\in\mathbb{Z}$ such that

$$1=gcd(a,b)=ax_0+by_0=ax_0-b(-y_0)$$

According to Division Algorithm, set

$$x_0=k_1\cdot b+r_1 \qquad k_1,r_1\in\mathbb{Z}, 0\leqslant r_1<b$$

$$-y_0=k_2\cdot a+r_2 \qquad k_2,r_2\in\mathbb{Z}, 0\leqslant r_2<a$$

Set $m=max\{-k_1,-k_2\}, n=min\{-k_1-1,-k_2-1\}$, then since $a,b\in\mathbb{N}\backslash\{0\}, \forall k\geqslant m, k\in\mathbb{Z}$

$$x_0+kb\geqslant x_0+mb\geqslant k_1b+r_1+(-k_1)b=r_1\geqslant 0$$

$$-y_0+ka\geqslant -y_0+ma\geqslant k_2a+r_2+(-k_2)a=r_2\geqslant 0$$

And $\forall k\leqslant n, k\in\mathbb{Z}$

$$x_0+kb\leqslant x_0+nb\leqslant k_1b+r_1+(-k_1-1)b=r_1-b<0$$

$$-y_0 + ka \leqslant -y_0 + na \leqslant k_2 a + r_2 + (-k_2 - 1)a = r_2 - a < 0$$

Then if $c \geqslant 0$, $\forall k \geqslant m$, $c(x_0 + kb), c(-y_0 + ka) \in \mathbb{N}$,

$$a(c(x_0 + kb)) - b(c(-y_0 + ka)) = c(ax_0 + by_0) = c$$

if $c < 0$, $\forall k \leqslant n$, $c(x_0 + kb), c(-y_0 + ka) \in \mathbb{N}$,

$$a(c(x_0 + kb)) - b(c(-y_0 + ka)) = c(ax_0 + by_0) = c$$

so $\forall c \in \mathbb{Z}$, there exist infinitely many solutions $x, y \in \mathbb{N}$ of the Diophantine equation $ax - by = c$.

8.2

$$\begin{aligned}
-158 &= -3 \cdot 57 + 13 \\
57 &= 4 \cdot 13 + 5 \\
13 &= 2 \cdot 5 + 3 \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

So according to The Euclidean Algorithm, $gcd(-158, 57) = 1$. And $-158 \cdot (-154) + 57 \cdot (-427) = -7$, so $x = -154, y = -427$ is a solution of $-158x + 57y = -7$, i.e.$158x - 57y = 7, x, y \in \mathbb{Z}$. So all the solutions are

$$x = -154 + \frac{-57}{1}t = -154 - 57t, y = -427 - \frac{158}{1}t = -427 - 158t, t \in \mathbb{Z}$$

To find all solution in $\mathbb{N}$, let $x \geqslant 0, y \geqslant 0$, we get that

$$\begin{cases} -154 - 57t \geqslant 0 \\ -427 - 158t \geqslant 0 \end{cases} \Rightarrow t \leqslant -427/158 \approx -2.7$$

To sum up, all $x, y \in \mathbb{N}$ such that $158x - 57y = 7$ are

$$x = -154 - 57t, y = -427 - 158t, t \leqslant -3, t \in \mathbb{Z}$$

9

9.1

Proof: Use induction to prove

1. When $k = 0$, $n = 3k + 1 = 1$ which cannot be factored into two smaller integers each of which belongs to S. So 1 is a prime and the statement holds.

2. Assume that when $k \leqslant m$ the statement holds, then for $k = m + 1$

   (a) $3(m + 1) + 1$ is a prime

   (b) $3(m + 1) + 1$ can be factored into two smaller integers a, b each of which belongs to S. Then according to the assumption, a, b are either prime or a product of primes. Since $3(m + 1) + 1 = ab$, $3(m + 1) + 1$ is a product of primes.

   So $3(m + 1) + 1$ is either a prime or a product of primes. So the statement holds when $k = m + 1$

From 1.2., any member of S is either prime or a product of primes.

9.2

$$1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, \cdots$$

$3 \cdot 73 + 1 = 220 = 4 \cdot 55 = 10 \cdot 22$. We can see that 4,10,22,55 are all primes, so it is possible for an element of S to be factored into primes in more than one way.

10

10.1

Proof: Assume that $\exists k \in \mathbb{N}$, such that $4k + 3$ is a prime and $4k + 3|d$.

Since D is finite and p is the largest prime in D, $4k + 3 \in D$ and$(4k + 3)|(3 \cdot 7 \cdot \cdots \cdot p)$. So $(4k + 3)|(4 \cdot (3 \cdot 7 \cdot \cdots \cdot p) - d)$, i.e.$(4k + 3)|1$. So $4k + 3 = \pm 1$. Since $k \in \mathbb{N}$, this is impossible.

So no prime of the form $4 \cdot k + 3$ divides d.

10.2

First we know that $2|4k, 2|4k + 2$, while d is odd, so d doesn't have prime factors in the form of $4k, 4k + 2$. Since we have proved that no prime of the form $4 \cdot k + 3$ divides d, then if d is not a prime, it can only have the prime factor in the form of $4k + 1$. $\forall k_1, k_2 \in \mathbb{N}$,

$$(4k_1 + 1)(4k_2 + 1) = 4(4k_1k_2 + k_1 + k_2) + 1$$

so d is in the form of $4k + 1$. However, since $d = 4((3 \cdot 7 \cdot \cdots \cdot p) - 1) + 3$ is of the form $4k + 3$, this is contradiction.

So we can conclude that d is a prime, and therefore d is not divisible by $4 \cdot k + 1, k \in \mathbb{N}^*$.

10.3

We have seen that d is a prime in the form of $4k + 3$, and $d = 4((3 \cdot 7 \cdot \cdots \cdot p) - 1) + 3 > 4(2p - 1) + 3 = 8p - 1 > p$. So there exists some more primes of the form $4k + 3$ which are greater than p. While we have assumed that prime of the form $4k + 3$ is finite and p is the largest one, then it leads to contradition. So there is an infinite number of primes of the form $4 \cdot n + 3$.