MA1100 Homework 4

Qi Ji

A0167793L

T04

3rd November 2017

Q 1. **(a)** Show that for any $a, b, c, d \in \mathbb{N}$, if $a \mid b$ and $c \mid d$, then $ac \mid bd$.

Proof.

1. For any $a, b, c, d \in \mathbb{N}$ with $a \mid b$ and $c \mid d$, then the following holds,
$$\exists k_1 \in \mathbb{N}.\ a \cdot k_1 = b$$
$$\exists k_2 \in \mathbb{N}.\ c \cdot k_2 = d$$
2. then $bd = (ak_1) \cdot (ck_2) = (ac) \cdot (k_1 k_2)$, so $ac \mid bd$. $\square$

(b) Show that for any $a, b, c \in \mathbb{N}$ with $c > 0$, if $ac \mid bc$, then $a \mid b$.

Proof.

1. For any $a, b, c \in \mathbb{N}$ where $c > 0$, if $ac \mid bc$, then
$$\exists k \in \mathbb{N}.\ ac \cdot k = bc$$
2. Since $c \neq 0$, by cancellation property of $\cdot$, $ak = b$, so $a \mid b$. $\square$

Q 2. Show that for all $n \in \mathbb{N}$, the product $n(n^2 + 5)$ is divisible by 6.

Proof.

1. Consider the following subset of $\mathbb{N}$,
$$S := \left\{\, n \in \mathbb{N} : 6 \mid n(n^2 + 5) \,\right\}$$
2. Then $0 \in S$, because $6 \cdot 0 = 0 = 0(0^2 + 5)$ so $6 \mid 0(0^2 + 5)$.
3. For any $n \in S$, $6 \mid n(n^2 + 5)$ so $\exists k \in \mathbb{N}.\ 6 \cdot k = n(n^2 + 5)$, then
$$\begin{aligned}
(n+1)\left((n+1)^2 + 5\right) &= (n+1)(n^2 + 2n + 6) \\
&= n^3 + 2n^2 + 6n + n^2 + 2n + 6 \\
&= n^3 + 3n^2 + 8n + 6 \\
&= n^3 + 5n + 3n^2 + 3n + 6 \\
&= n(n^2 + 5) + 3 \cdot n(n+1) + 6 \\
(n+1)\left((n+1)^2 + 5\right) &= 6k + 3 \cdot n(n+1) + 6 \qquad (2.1)
\end{aligned}$$

Known Result. $n \in S \subseteq \mathbb{N}$ is even or odd.

(1). Case n is even, so $\exists l_1 \in \mathbb{N}.\ n = 2l_1$, then (2.1) can be rewritten as

$$\begin{aligned}(n+1)\left((n+1)^2+5\right) &= 6k + 3\cdot(2l_1)(n+1)+6 \\ &= 6k+6\cdot l_1(n+1)+6 \\ &= 6(k+l_1(n+1)+1)\end{aligned}$$

Hence $6 \mid (n+1)\left((n+1)^2+5\right)$ and $n+1 \in S$.

(2). Case n is odd, so $\exists l_2 \in \mathbb{N}.\ n = 2l_2+1$, then (2.1) can be rewritten as

$$\begin{aligned}(n+1)\left((n+1)^2+5\right) &= 6k + 3\cdot n(2l_2+1+1)+6 \\ &= 6k+6\cdot n(l_2+1)+6 \\ &= 6(k+n(l_2+1)+1)\end{aligned}$$

Hence $6 \mid (n+1)\left((n+1)^2+5\right)$ and $n+1 \in S$.

4. Therefore by induction, $S = \mathbb{N}$, for all $n \in \mathbb{N}$, $n(n^2+5)$ is divisible by 6. $\square$

Q 3. Show that for all $n \in \mathbb{N}$, the number $3n^7+7n^3+11n$ is divisible by 21.

Proof.

1. Consider the subset $S \subseteq \mathbb{N}$,

$$S := \left\{\, n \in \mathbb{N} : 21 \mid 3n^7+7n^3+11n \,\right\}$$

2. Then $0 \in S$, because $21\cdot 0 = 0 = 3\cdot 0^7+7\cdot 0^3+11\cdot 0$, which means $21 \mid 3\cdot 0^7+7\cdot 0^3+11\cdot 0$.

3. For any $n \in S$, $21 \mid 3n^7+7n^3+11n$, so $\exists k \in \mathbb{N}.\ 21\cdot k = 3n^7+7n^3+11n$, then

$$\begin{aligned}&3(n+1)^7+7(n+1)^3+11(n+1) \\ &= 3\left(n^7+7n^6+21n^5+35n^4+35n^3+21n^2+7n+1\right) \\ &\quad + 7\left(n^3+3n^2+3n+1\right)+11n+11 \\ &= 3n^7+21n^6+63n^5+105n^4+105n^3+63n^2+21n+3 \\ &\quad + 7n^3+21n^2+21n+7+11n+11 \\ &= 3n^7+21n^6+63n^5+105n^4+105n^3+84n^2+42n+21+7n^3+11n \\ &= 21k+21n^6+(21\cdot 3)n^5+(21\cdot 5)n^4+(21\cdot 5)n^3+(21\cdot 4)n^2+(21\cdot 2)n+21 \\ &= 21(k+n^6+3n^5+5n^4+5n^3+4n^2+2n+1)\end{aligned}$$

Hence $21 \mid 3(n+1)^7+7(n+1)^3+11(n+1)$, $n+1 \in S$.

4. Therefore by induction, $S = \mathbb{N}$, for all $n \in \mathbb{N}$, $3n^7+7n^3+11n$ is divisible by 21. $\square$

Q 4. Show that for any $n \in \mathbb{N}$, $n^2 + 2$ is not divisible by 4.

Proof.

1. *Base cases.*

$$\begin{aligned} 0^2 + 2 = 2 = 4 \cdot 0 + 2 &\implies 4 \nmid 2 \\ 1^2 + 2 = 3 = 4 \cdot 0 + 3 &\implies 4 \nmid 3 \end{aligned}$$

2. *Induction step.* For any $n \in \mathbb{N}$ where $4 \nmid n^2 + 2$,

$$\exists q \in \mathbb{N}, r \in \{ 1, 2, 3 \} .\ n^2 + 2 = 4 \cdot q + r$$

then $4 \nmid (n+2)^2 + 2$, because

$$\begin{aligned} (n+2)^2 + 2 &= n^2 + 4n + 4 + 2 \\ &= 4q + r + 4n + 4 \\ &= 4q + 4n + 4 + r \\ &= 4(q + n + 1) + r \end{aligned}$$

3. Since $q + n + 1 \in \mathbb{N}$ and $r \in \{ 1, 2, 3 \}$, by division algorithm $4 \nmid (n+2)^2 + 2$.

4. Therefore by induction, $n^2 + 2$ is not divisible by 4 for all $n \in \mathbb{N}$. □

Q 5. Show that if $m, n \in \mathbb{N}$ are odd natural numbers, then $m^2 + n^2$ is even but not divisible by 4.

Proof.

1. $m, n \in \mathbb{N}$ are odd, so $\exists k, l \in \mathbb{N}.\ m = 2k + 1, n = 2l + 1$, then

$$\begin{aligned} m^2 + n^2 &= (2k+1)^2 + (2l+1)^2 \\ &= 4k^2 + 4k + 1 + 4l^2 + 4l + 1 \\ &= 2(2k^2 + 2l^2 + 2k + 2l + 1) && (5.1) \\ &= 4(k^2 + l^2 + k + l) + 2 && (5.2) \end{aligned}$$

2. From (5.1), since $k^2 + l^2 + 2k + 2l + 1 \in \mathbb{N}$, $m^2 + n^2$ is even.

3. By division algorithm on $m^2 + n^2$ with $d = 4$, from (5.2), we see that the (uniquely determined) $q = k^2 + l^2 + k + l \in \mathbb{N}$ and $r = 2$, in particular, $r \neq 0$, so $4 \nmid m^2 + n^2$. □

Q 6. Determine how many natural numbers $n \in \mathbb{N}$ with $100 \leq n \leq 1000$ are divisible by 7.

1. The set of all natural numbers $n \in \mathbb{N}$ in $100 \leq n \leq 1000$ where $7 \mid n$ is

$$S := \left\{\begin{array}{l} 105, 112, 119, 126, 133, 140, 147, 154, 161, 168, 175, 182, 189, 196, \\ 203, 210, 217, 224, 231, 238, 245, 252, 259, 266, 273, 280, 287, 294, \\ 301, 308, 315, 322, 329, 336, 343, 350, 357, 364, 371, 378, 385, 392, 399, \\ 406, 413, 420, 427, 434, 441, 448, 455, 462, 469, 476, 483, 490, 497, \\ 504, 511, 518, 525, 532, 539, 546, 553, 560, 567, 574, 581, 588, 595, \\ 602, 609, 616, 623, 630, 637, 644, 651, 658, 665, 672, 679, 686, 693, \\ 700, 707, 714, 721, 728, 735, 742, 749, 756, 763, 770, 777, 784, 791, 798, \\ 805, 812, 819, 826, 833, 840, 847, 854, 861, 868, 875, 882, 889, 896, \\ 903, 910, 917, 924, 931, 938, 945, 952, 959, 966, 973, 980, 987, 994 \end{array}\right\}$$

2. It can be verified that

$$\begin{array}{llllllll}
7 \cdot 15 & = 105 & 7 \cdot 42 & = 294 & 7 \cdot 69 & = 483 & 7 \cdot 96 & = 672 \\
7 \cdot 16 & = 112 & 7 \cdot 43 & = 301 & 7 \cdot 70 & = 490 & 7 \cdot 97 & = 679 \\
7 \cdot 17 & = 119 & 7 \cdot 44 & = 308 & 7 \cdot 71 & = 497 & 7 \cdot 98 & = 686 \\
7 \cdot 18 & = 126 & 7 \cdot 45 & = 315 & 7 \cdot 72 & = 504 & 7 \cdot 99 & = 693 \\
7 \cdot 19 & = 133 & 7 \cdot 46 & = 322 & 7 \cdot 73 & = 511 & 7 \cdot 100 & = 700 \\
7 \cdot 20 & = 140 & 7 \cdot 47 & = 329 & 7 \cdot 74 & = 518 & 7 \cdot 101 & = 707 \\
7 \cdot 21 & = 147 & 7 \cdot 48 & = 336 & 7 \cdot 75 & = 525 & 7 \cdot 102 & = 714 \\
7 \cdot 22 & = 154 & 7 \cdot 49 & = 343 & 7 \cdot 76 & = 532 & 7 \cdot 103 & = 721 \\
7 \cdot 23 & = 161 & 7 \cdot 50 & = 350 & 7 \cdot 77 & = 539 & 7 \cdot 104 & = 728 \\
7 \cdot 24 & = 168 & 7 \cdot 51 & = 357 & 7 \cdot 78 & = 546 & 7 \cdot 105 & = 735 \\
7 \cdot 25 & = 175 & 7 \cdot 52 & = 364 & 7 \cdot 79 & = 553 & 7 \cdot 106 & = 742 \\
7 \cdot 26 & = 182 & 7 \cdot 53 & = 371 & 7 \cdot 80 & = 560 & 7 \cdot 107 & = 749 \\
7 \cdot 27 & = 189 & 7 \cdot 54 & = 378 & 7 \cdot 81 & = 567 & 7 \cdot 108 & = 756 \\
7 \cdot 28 & = 196 & 7 \cdot 55 & = 385 & 7 \cdot 82 & = 574 & 7 \cdot 109 & = 763 \\
7 \cdot 29 & = 203 & 7 \cdot 56 & = 392 & 7 \cdot 83 & = 581 & 7 \cdot 110 & = 770 \\
7 \cdot 30 & = 210 & 7 \cdot 57 & = 399 & 7 \cdot 84 & = 588 & 7 \cdot 111 & = 777 \\
7 \cdot 31 & = 217 & 7 \cdot 58 & = 406 & 7 \cdot 85 & = 595 & 7 \cdot 112 & = 784 \\
7 \cdot 32 & = 224 & 7 \cdot 59 & = 413 & 7 \cdot 86 & = 602 & 7 \cdot 113 & = 791 \\
7 \cdot 33 & = 231 & 7 \cdot 60 & = 420 & 7 \cdot 87 & = 609 & 7 \cdot 114 & = 798 \\
7 \cdot 34 & = 238 & 7 \cdot 61 & = 427 & 7 \cdot 88 & = 616 & 7 \cdot 115 & = 805 \\
7 \cdot 35 & = 245 & 7 \cdot 62 & = 434 & 7 \cdot 89 & = 623 & 7 \cdot 116 & = 812 \\
7 \cdot 36 & = 252 & 7 \cdot 63 & = 441 & 7 \cdot 90 & = 630 & 7 \cdot 117 & = 819 \\
7 \cdot 37 & = 259 & 7 \cdot 64 & = 448 & 7 \cdot 91 & = 637 & 7 \cdot 118 & = 826 \\
7 \cdot 38 & = 266 & 7 \cdot 65 & = 455 & 7 \cdot 92 & = 644 & 7 \cdot 119 & = 833 \\
7 \cdot 39 & = 273 & 7 \cdot 66 & = 462 & 7 \cdot 93 & = 651 & 7 \cdot 120 & = 840 \\
7 \cdot 40 & = 280 & 7 \cdot 67 & = 469 & 7 \cdot 94 & = 658 & 7 \cdot 121 & = 847 \\
7 \cdot 41 & = 287 & 7 \cdot 68 & = 476 & 7 \cdot 95 & = 665 & 7 \cdot 122 & = 854
\end{array}
\quad
\begin{array}{ll}
7 \cdot 123 & = 861 \\
7 \cdot 124 & = 868 \\
7 \cdot 125 & = 875 \\
7 \cdot 126 & = 882 \\
7 \cdot 127 & = 889 \\
7 \cdot 128 & = 896 \\
7 \cdot 129 & = 903 \\
7 \cdot 130 & = 910 \\
7 \cdot 131 & = 917 \\
7 \cdot 132 & = 924 \\
7 \cdot 133 & = 931 \\
7 \cdot 134 & = 938 \\
7 \cdot 135 & = 945 \\
7 \cdot 136 & = 952 \\
7 \cdot 137 & = 959 \\
7 \cdot 138 & = 966 \\
7 \cdot 139 & = 973 \\
7 \cdot 140 & = 980 \\
7 \cdot 141 & = 987 \\
7 \cdot 142 & = 994
\end{array}$$

3. By counting, $|S| = 128$. $\square$

Definition. A *perfect square* is a natural number $n \in \mathbb{N}$ such that there exists $k \in \mathbb{N}$ for which $n = k^2$.

Q 7. Show that if $m, n \in \mathbb{N}$ are odd natural numbers, then $m^2 + n^2$ is not a perfect square.

Proof.

1. Given 2 odd natural numbers $m, n \in \mathbb{N}$, $\exists a, b \in \mathbb{N}.\ m = 2a+1, n = 2b+1$, then

$$\begin{aligned} m^2 + n^2 &= (2a+1)^2 + (2b+1)^2 \\ &= 4a^2 + 4a + 1 + 4b^2 + 4b + 1 \\ &= 4a^2 + 4b^2 + 4a + 4b + 2 \\ m^2 + n^2 &= 2(2a^2 + 2b^2 + 2a + 2b + 1) \qquad (7.1) \\ m^2 + n^2 &= 4(a^2 + a + b^2 + b) + 2 \qquad (7.2) \end{aligned}$$

2. Suppose for a contradiction $\exists k \in \mathbb{N}.\ k^2 = m^2 + n^2$, from (7.1)

$$k^2 = 2(2a^2 + 2b^2 + 2a + 2b + 1)$$

   in particular, $k^2 > 0$ and k^2 is even.

   Claim. k is even.

   - If not, $\exists l \in \mathbb{N}.\ k = 2l + 1$, then

$$\begin{aligned} k^2 &= (2l+1)^2 \\ &= 4l^2 + 4l + 1 \\ &= 2(2l^2 + 2l) + 1 \end{aligned}$$

   - implying k^2 is odd, a contradiction

3. So k is even, then $\exists c \in \mathbb{N}.\ k = 2c$, which implies $k^2 = 4c^2$, in particular, $4 \mid k^2$.

4. But from (7.2),

$$k^2 = 4(a^2 + a + b^2 + b) + 2$$

   by division algorithm applied on k^2 with $d = 4$, get $q = a^2 + a + b^2 + b \in \mathbb{N}$ and $r = 2$, which means in particular, $4 \nmid k^2$, a contradiction.

5. Therefore, for any odd $m, n \in \mathbb{N}$, there does not exist $k \in \mathbb{N}$ where $k^2 = m^2 + n^2$, and $m^2 + n^2$ is not a perfect square. □

Q 8. Show that if $m, n \in \mathbb{N}$ are natural numbers not divisible by 3, then $m^2 + n^2$ is not a perfect square.

Proof.

1. Given $m, n \in \mathbb{N}$, suppose for a contradiction $m^2 + n^2$ is a perfect square, where $\exists k \in \mathbb{N}$ such that $m^2 + n^2 = k^2$.

2. Apply division algorithm on k with $d = 3$, we have

$$k = 3q_k + r_k$$

   where $q_k \in \mathbb{N}$ and $r_k \in \{0, 1, 2\}$ are uniquely determined by k.

3. Since $3 \nmid m$ and $3 \nmid n$, repeating the division algorithm,

$$\begin{aligned} m &= 3q_m + r_m \\ n &= 3q_n + r_n \end{aligned}$$

   where $q_m, q_n \in \mathbb{N}$ and $r_m, r_n \in \{1, 2\}$ are uniquely determined by m, n respectively.

4. Since $m^2 + n^2$ is a perfect square,

$$\begin{aligned} m^2 + n^2 &= k^2 \\ (3q_m + r_m)^2 + (3q_n + r_n)^2 &= (3q_k + r_k)^2 \\ 9q_m^2 + 6q_m r_m + r_m^2 + 9q_n^2 + 6q_n r_n + r_n^2 &= 9q_k^2 + 6q_k r_k + r_k^2 \\ 3(3q_m^2 + 2q_m r_m + 3q_n^2 + 2q_n r_n) + r_m^2 + r_n^2 &= 3(3q_k^2 + 2q_k r_k) + r_k^2 \end{aligned} \tag{8.1}$$

5. For readability, define $e_1, e_2 \in \mathbb{N}$ and rewrite (8.1)

$$\begin{aligned} e_1 &:= 3q_m^2 + 2q_m r_m + 3q_n^2 + 2q_n r_n \\ e_2 &:= 3q_k^2 + 2q_k r_k \\ 3e_1 + r_m^2 + r_n^2 &= 3e_2 + r_k^2 \end{aligned} \tag{8.2}$$

6. By enumerating possible values, $r_m^2 + r_n^2 \in \{2, 5, 8\}$, $r_k^2 \in \{0, 1, 4\}$

7. When applying division algorithm on LHS of (8.2) with $d = 3$,

$$\begin{aligned} m^2 + n^2 &= 3e_1 + 2 \text{ or} \\ m^2 + n^2 &= 3e_1 + 5 = 3(e_1 + 1) + 2 \text{ or} \\ m^2 + n^2 &= 3e_1 + 8 = 3(e_1 + 2) + 2 \end{aligned}$$

   In any case, LHS has $r = 2$ when applied division algorithm with $d = 3$

8. However, when applying division algorithm on RHS of (8.2) with $d = 3$,

$$\begin{aligned} k^2 &= 3e_2 \text{ or} \\ k^2 &= 3e_2 + 1 \text{ or} \\ k^2 &= 3e_2 + 4 = 3(e_2 + 1) + 1 \end{aligned}$$

   In no case does RHS have $r = 2$, a contradiction.

9. Hence for any $m, n \in \mathbb{N}$ not divisible by 3, $m^2 + n^2$ is not a perfect square. $\square$

Q 9. (a) Let $n \in \mathbb{N}$. Prove or disprove: if there exists a prime number p such that $2^n = p+1$, then n is prime.

Proof.

1. If prime number p exists, such that $2^n = p + 1$ where $n \in \mathbb{N}$.
2. Since $2^0 = 0 + 1$ and 0 is not prime, $n \neq 0$.
3. Suppose for contradiction n is not prime, so $\exists a, b \in \mathbb{N}.\ n = a(b+1), a > 1, b > 0$, then
$$2^n = 2^{a(b+1)} = p + 1$$
take $d \in \mathbb{N}$ to be the number where $d + 1 = 2^a$.
4. Consider the sum
$$\sum_{i=0}^{b+1} 2^{ai} = 1 + \sum_{i=1}^{b+1} 2^{ai}$$
LHS: expand by definition; RHS: factor 2^a from every term in the summation
$$2^{a(b+1)} + \sum_{i=0}^{b} 2^{ai} = 1 + 2^a \sum_{i=0}^{b} 2^{ai}$$
$$p + 1 + \sum_{i=0}^{b} 2^{ai} = 1 + (d+1) \sum_{i=0}^{b} 2^{ai}$$
$$p + \sum_{i=0}^{b} 2^{ai} = (d+1) \sum_{i=0}^{b} 2^{ai}$$
$$p + \sum_{i=0}^{b} 2^{ai} = d \sum_{i=0}^{b} 2^{ai} + \sum_{i=0}^{b} 2^{ai}$$
$$p = d \sum_{i=0}^{b} 2^{ai}$$
5. so $d \mid p$, but because $a > 1$,
$$2^a > 2$$
$$d > 1$$
and because $b > 0$
$$\sum_{i=0}^{b} 2^{ai} \geq 1 + 2^a > 1$$
6. Contradicting primality of p. $\square$

(b) Let $n \in \mathbb{N}$. Prove or disprove: if n is prime, then there exists a prime number p such that $2^n = p + 1$.

False. Take $n = 109$ which is prime, then

$$\begin{aligned} 2^{109} &= 649037107316853453566312041152512 \\ &= 649037107316853453566312041152511 + 1 \\ &= (745988807 \cdot 870035986098720987332873) + 1 \end{aligned}$$

Q 10. **(a)** Let $n \in \mathbb{N}$. Prove or disprove: if $2^n + 1$ is prime, then there exists $k \in \mathbb{N}$ such that $n = 2^k$.

False. Take $n = 0 \in \mathbb{N}$,

$$2^0 + 1 = 1 + 1 = 2$$

is prime, but there does not exists $k \in \mathbb{N}$ where $2^k = 0$.

(b) Let $n \in \mathbb{N}$. Prove or disprove: if there exists $k \in \mathbb{N}$ such that $n = 2^k$, then $2^n + 1$ is prime.
False. Take $n = 2^7 = 128$, then

$$\begin{aligned} 2^{128} + 1 &= 340282366920938463463374607431768211456 + 1 \\ &= 340282366920938463463374607431768211457 \\ &= 59649589127497217 \cdot 5704689200685129054721 \end{aligned}$$

Q 11. Let p be a prime number. Show that if there exists $k \in \mathbb{N}$ such that $p = 3k + 1$, then there exists $n \in \mathbb{N}$ such that $p = 6n + 1$.

Proof.

1. Let p be a prime number, suppose there exists $k \in \mathbb{N}$ such that $p = 3k + 1$.
2. Consider the case k is odd, so $\exists l \in \mathbb{N}.\ 2l + 1 = k$, then

$$p = 3(2l + 1) + 1 = 6l + 4 = 2(3l + 2)$$

have $2 \mid p$ and $p \geq 4 \implies p \neq 2$, contradicting primality of p. So k cannot be odd.

3. Hence k is even, $\exists n \in \mathbb{N}.\ 2n = k$, then

$$p = 3(2n) + 1 = 6n + 1.$$

So $n \in \mathbb{N}$ exists. $\square$

Q 12. Show that for any $n \in \mathbb{N}$ such that there exists $k \in \mathbb{N}$ such that $n = 3k + 2$, there exists a prime number $d \in \mathbb{N}$ such that $d \mid n$ and there exists $k' \in \mathbb{N}$ such that $d = 3k' + 2$.

Proof.

1. For any $n \in \mathbb{N}$, suppose there exists $k \in \mathbb{N}$ such that $n = 3k + 2$.
2. Consider the subset $D \subseteq \mathbb{N}$,

$$D := \{ d \in \mathbb{N} : d \mid n \wedge (\exists k' \in \mathbb{N}.\ d = 3k' + 2) \}$$

3. Clearly $n \in D$, as $n \mid n$ and $n = 3k + 2$, so in particular, $D \neq \emptyset$.
4. By well-ordering principle, D has smallest element $d_0 = 3k_0 + 2$.

   Claim. d_0 is prime.

   (1). If not, $\exists a, b \in \mathbb{N}.\ a \neq 1, b \neq 1, d_0 = ab$,

$$d_0 = ab = 3k_0 + 2 \tag{12.1}$$

   (2). Apply division algorithm on a and b with divisor 3,

$$\begin{aligned} a &= \alpha \cdot 3 + \beta \\ b &= \gamma \cdot 3 + \delta \end{aligned}$$

   where $\alpha, \gamma \in \mathbb{N}$ and $\beta, \delta \in \{ 0, 1, 2 \}$ are uniquely determined by a, b respectively.

   (3). rewrite (12.1)

$$\begin{aligned} d_0 = 3k_0 + 2 &= (3\alpha + \beta)(3\gamma + \delta) \\ &= 9\alpha\gamma + 3\alpha\delta + 3\beta\gamma + \beta\delta \\ 3k_0 + 2 &= 3(3\alpha\gamma + \alpha\delta + \beta\gamma) + \beta\delta \end{aligned} \tag{12.2}$$

   (4). By enumeration of possibilities, $\beta\delta \in \{ 0, 1, 2, 4 \}$, then for (12.2) to be consistent when applied division algorithm with divisor 3, $\beta\delta = 2$.

   (5). Without loss of generality, assume $\beta = 2, \delta = 1$, then

$$a = 3\alpha + 2, \alpha \in \mathbb{N}$$

   also notice that $a \mid d_0$ and $d_0 \mid n$, so $a \mid n$ and as a result $a \in D$.

   (6). However, from (12.1), $a \mid d_0 \implies a \leq d_0$, but $b \neq 1$ so we have $a \neq d_0$, then $a < d_0$, contradicting with d_0 being smallest in D.

5. Hence $d_0 \in \mathbb{N}$ is a prime satisfying $d_0 \mid n$ and $\exists k' \in \mathbb{N}.\ d_0 = 3k' + 2$. □