# Solution 1

Arithmetic, Zorn's Lemma.

1. (a) Using the Euclidean division, determine $\gcd(1602, 399)$.
   (b) Find $m_0, n_0 \in \mathbb{Z}$ such that $\gcd(1602, 399) = 1602m_0 + 399n_0$. [*Hint:* Write the steps of the euclidean algorithm and compute 'backwards'.]
   (c) Similarly, determine $\gcd(123456, 876)$ and find $m_0, n_0 \in \mathbb{Z}$ such that
   $$\gcd(123456, 876) = 123456m_0 + 876n_0.$$
   (d) Determine $\gcd(\ell^2 + \ell + 1, 3\ell^2 + 4\ell + 5)$ for each $\ell \in \mathbb{Z}$.

   *Solution*:

   (a) We perform the Euclidean division of 1602 by 399. Then we divide 399 by the remainder and so on:
   $$\begin{aligned} 1602 &= 4 \cdot 399 + 6 \\ 399 &= 66 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$
   Then
   $$\gcd(1602, 399) = \gcd(399, 6) = \gcd(6, 3) = \gcd(3, 0) = 3.$$
   (b) By looking at the computations done in part (b), we obtain:
   $$3 = 399 - 66 \cdot 6 = 399 - 66 \cdot (1602 - 4 \cdot 399) = 265 \cdot 399 - 66 \cdot 1602.$$
   (c) We compute
   $$\begin{aligned} 123456 &= 140 \cdot 876 + 816 \\ 876 &= 816 + 60 \\ 816 &= 13 \cdot 60 + 36 \\ 60 &= 36 + 24 \\ 36 &= 24 + 12 \\ 24 &= 2 \cdot 12, \end{aligned}$$
   which implies that $\gcd(123456, 876) = 12$. Then we express 12 by looking at the above equations backwards:
   $$\begin{aligned} 12 &= 36 - 24 = 36 - (60 - 36) = -60 + 2 \cdot 36 = -60 + 2 \cdot (816 - 13 \cdot 60) \\ &= 2 \cdot 816 - 27 \cdot 60 = 2 \cdot 816 - 27 \cdot (876 - 816) = 29 \cdot 816 - 27 \cdot 876 \\ &= 29 \cdot (123456 - 1401 \cdot 876) - 27 \cdot 876 = 29 \cdot 123456 - 4087 \cdot 876. \end{aligned}$$

(d) We compute:

$$\begin{aligned} 3\ell^2+4\ell+5 &= 3\cdot(\ell^2+\ell+1)+(\ell+2)\\ \ell^2+\ell+1 &= (\ell-1)(\ell+2)+3. \end{aligned}$$

This implies that

$$\gcd(3\ell^2+4\ell+5,\ell^2+\ell+1)=\gcd(\ell^2+\ell+1,\ell+2)=\gcd(\ell+2,3).$$

Since 3 is a prime number, the greatest common divisor is either equal to 3 (if $3\mid \ell+2$) or 1 (if $3\nmid \ell+2$). Hence we can conclude that

$$\gcd(3\ell^2+4\ell+5,\ell^2+\ell+1)=\begin{cases} 1 & \text{if } \ell\equiv 0,2 \pmod 3\\ 3 & \text{if } \ell\equiv 1 \pmod 3). \end{cases}$$

2. A *Pythagorean triple* is an ordered triple $(a,b,c)$ of positive integers for which $a^2+b^2=c^2$. It is called *primitive* if $a,b$ and $c$ are *coprime*, that is, if there is no integer $d>1$ which divides $a$, $b$ and $c$.

(a) Let $1\leqslant x<y$ be odd integers. Prove that

$$\left(xy,\frac{y^2-x^2}{2},\frac{y^2+x^2}{2}\right) \tag{1}$$

is a Pythagorean triple.

(b) Suppose that $x$ and $y$ are also coprime. Prove that the Pythagorean triple (1) is primitive.

*(c) Prove that all primitive Pythagorean triples are of the form (1) with coprime odd integers $1\leqslant x<y$, up to switching the first two entries. [*Hint:* Reduce to the case in which $a$ is odd. Prove that $\frac{c+b}{a}\frac{c-b}{a}=1$ and write down $\frac{c+b}{a}=\frac{u}{t}$ and $\frac{c-b}{a}=\frac{t}{u}$ for coprime positive integers $u>t$. Find $\frac{c}{a}$ and $\frac{b}{a}$ in terms of $t$ and $u$.]

*Solution*:

(a) First, we notice that (1) consists of positive integers. Indeed, $xy\in\mathbb{Z}_{>0}$ as it is the product of two positive integers, whereas $x^2$ and $y^2$ are odd numbers because they are powers of odd numbers (e.g., the prime number 2 cannot divide the integer $x^2$ without dividing $x$), so that $y^2+x^2$ and $y^2-x^2$ are even numbers and the given fractions in (1) represent integers. It is also clear that both numbers are positive as $y>x>0$. Now we only need to check that the identity $a^2+b^2=c^2$ is satisfied for $(a,b,c)=\left(xy,\frac{y^2-x^2}{2},\frac{y^2+x^2}{2}\right)$. This can be done as follows:

$$a^2+b^2=x^2y^2+\frac{y^4+2x^2y^2+x^4}{4}=\frac{y^4-2x^2y^2+x^4}{4}=\frac{(y^2-x^2)^2}{4}=c^2.$$

(b) This is equivalent to check that for each prime number $p$ there is an entry in (1) which is not divided by $p$.

For $p = 2$ this is the case because $xy$ is odd by assumption (as $x$ and $y$ are both odd). Now assume by contraddiction that an odd prime $p$ divides all the entries in (1). Then $p$ divides $y^2 + x^2$, because it divides $\frac{y^2+x^2}{2}$. Moreover $p|xy$, which implies that $p|x$ or $p|y$. If $p|x$, then $p|x^2$, so that it also divides $(y^2 + x^2) - x^2 = y^2$ and being $p$ prime it must divide $y$. If $p|y$ we similarly show that $p|x$. In any case, $p$ divides both $x$ and $y$, which is a contradiction to the assumption that $x$ and $y$ are coprime. Hence $p$ cannot divide all the entries in (1) simultaneously, as we wanted to show.

(c) Let $(a, b, c)$ be a primitive Pythagorean triple.

Suppose that $a$ and $b$ are both even. Then $c^2 = a^2+b^2$ is even, too. This implies that $c$ is even, contradicting the hypothesis that $(a, b, c)$ is primitive. Hence at least one among the numbers $a$ and $b$ is odd and since we are allowed to switch the first two entries in the Pythagorean triple, we can assume WLOG that this is $a$.

The equality $a^2 + b^2 = c^2$ is equivalent to $1 = \frac{c^2}{a^2} - \frac{b^2}{a^2}$ which reads

$$\frac{c+b}{a} \cdot \frac{c-b}{a} = 1. \tag{2}$$

Since $\frac{c+b}{a} > 0$, we can write $\frac{c+b}{a} = \frac{u}{t}$ for coprime positive integers $u$ and $t$. Notice that $c^2 = a^2 + b^2 > a^2$, implying that $c > a$ so that $c + b > c > a$ and $u > t$. Moreover, (2) implies that $\frac{c-b}{a} = \frac{t}{u}$. Summing and subtracting the two equations

$$\frac{c+b}{a} = \frac{u}{t}$$
$$\frac{c-b}{a} = \frac{t}{u}$$

we obtain

$$\frac{b}{a} = \frac{u^2 - t^2}{2ut}$$
$$\frac{c}{a} = \frac{u^2 + t^2}{2ut}$$

Notice that primitivity of $(a, b, c)$ implies that $\gcd(a, c) = 1$, because any common prime factor of $a$ and $c$ would divide $b^2 = c^2 - a^2$ and hence $b$. Similarly $\gcd(a, b) = 1$. Moreover, since $a$ is odd, 2 must divide $u^2 - t^2$ and $u^2+t^2$. Now the same argument as in part (b) gives $\gcd(ut, \frac{u^2+t^2}{2}) = 1$ because $u$ and $t$ are coprime, and similarly we get $\gcd(ut, \frac{u^2-t^2}{2}) = 1$.

The only possibility is that $a = ut$, $c = \frac{u^2+t^2}{2}$ and $b = \frac{u^2-t^2}{2}$, so that we can conclude by taking $x = u$ and $y = v$.

3. In this exercise we give a famous proof by Zagier of Fermat's theorem on sums of two squares. For $m, n, r \in \mathbb{Z}$ we say that $m$ is *congruent to $r$ modulo $n$*, and write $m \equiv r \pmod{n}$, if $m - r \in n\mathbb{Z}$.

   **Theorem 0.1** (Fermat)**.** *Let $p$ be an odd prime number. Then it is possible to express $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 (\mathit{mod}\ 4)$.*

   Let $X$ be a set. An *involution* of $X$ is a map $\varphi : X \longrightarrow X$ such that $\varphi \circ \varphi = \mathrm{id}_X$.

   (a) Prove: if $X$ is finite and has odd cardinality, then every involution of $X$ has a fixed point.

   (b) Prove: if $X$ is finite and an involution of $X$ has a unique fixed point, then $|X|$ is odd.

   In parts (c)-(f), suppose that $p \equiv 1 \pmod 4$ is a prime number. Let

$$X_p := \{(x, y, z) \in \mathbb{Z}^3_{\geqslant 0} : x^2 + 4yz = p\}.$$

   (c) Show that $X_p$ is finite and non-empty.

   (d) Show that the maps $f, g : X_p \longrightarrow X_p$ sending

$$f : (x, y, z) \longmapsto \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

$$g : (x, y, z) \longmapsto (x, z, y)$$

   are well defined involutions.

   (e) Let $A = \{(x, y, z) \in X_p : x < y - z\}$, $B = \{(x, y, z) \in X_p : y - z < x < 2y\}$ and $C = \{(x, y, z) \in X_p : x > 2y\}$. Prove that $f(A) \subseteq C$ and $f(C) \subseteq A$. Deduce that $f(B) \subseteq B$ and use this to prove that $f$ has a unique fixed point.

   (f) Deduce that $|X_p|$ is odd and conclude that the "if" statement holds.

   (g) Prove that if $p = x^2 + y^2$ for $x, y \in \mathbb{Z}$, then $p \equiv 1 (\mathrm{mod}\ 4)$.

   *Solution*:

   (a) Let $\varphi$ be an involution of $X$. Denote by $X^\varphi$ the set of fixed points of $X$, i.e. $X^\varphi := \{x \in X : \varphi(x) = x\}$. Then

$$X = X^\varphi \sqcup \{x \in X : \varphi(x) \neq x\}. \tag{3}$$

   The set $Y := \{x \in X : \varphi(x) \neq x\}$ has even cardinality, as can be checked by induction on its cardinality:

   - If $Y = \varnothing$, then $|Y| = 0$ is even and we are done.

- Else fix $y_0 \in Y$. Notice that $\varphi(Y) \subseteq Y$ as for $y \in Y$ one can observe that $\varphi(\varphi(y)) = y \neq \varphi(y)$, so that $\varphi(y) \in Y$. Moreover, $\varphi$ being an involution, we see that $\{y_0, \varphi(y_0)\}$ is mapped to itself by $\varphi$ and so is $Y' := Y \smallsetminus \{y_0, \varphi(y_0)\}$ again because $\varphi$ is an involution. Now consider the involution $\varphi'$ of $X$ given by

$$\varphi'(x) = \begin{cases} \varphi(x) & x \notin \{y_0, \varphi(y_0)\} \\ x & x \in \{y_0, \varphi(y_0)\}. \end{cases}$$

  We have $X^{\varphi'} = X^{\varphi} \sqcup \{y_0, \varphi(y_0)\}$ so that $\{x \in X : \varphi'(x) \neq x\} = Y'$ has cardinality $|Y'| = |Y| - 2 < |Y|$ which by inductive hypothesis has even cardinality. Hence $|Y'|$ has even cardinality as well.

Now if $|X|$ is even, then $|X^{\varphi}|$ must be odd by what we have just showed and (3), so that it cannot be empty. This means that there exists a fixed point.

(b) If $\varphi$ has a unique fixed point, then $|X^{\varphi}| = 1$ is odd. Since $\{x \in X : \varphi(x) \neq x\}$ has even cardinality as seen in (a), equation (3) implies that $|X|$ is odd.

(c) First of all, notice that for $(x, y, z) \in X_p$ one has $x \neq 0$, $y \neq 0$ and $z \neq 0$. Indeed, if $x = 0$ then $4yz = p$, whereas for $y = 0$ or $z = 0$ we obtain $x^2 = p$, and both conclusions are impossible since $p$ is prime. Then $x, y, z$ are all smaller than $x^2 + 4yz = p$, so that they all lie in the set $\{1, \dots, p\}$. Hence $X_p$ is finite with at most $p^3$ elements. Writing $p = 1 + 4k$, we see that $(1, 1, k) \in X_p$ which in turn is non-empty.

(d) Clearly, for $(x, y, z) \in X_p$ one has $(x, z, y) \in X_p$ and

$$g^2(x, y, z) = g(x, z, y) = (x, y, z)$$

so that $g$ is a well defined involution.

Let's now deal with $f$. First notice that the three stated cases are disjoint and cover all the possibilities: the equalities of coordinates $x = y - z$ and $x = 2y$ are both impossible for $(x, y, z) \in X_p$. The former implies $p = x^2 + 4yz = (y + z)^2$ whereas the latter implies that $p = x^2 + 4yz = 4y(y + z)$ and both conclusions are a contradiction with primality of $p$. We use the claim from the next point that $f$ switches $A$ and $C$ and that it fixes $B$, which we prove later together with the fact that $\varphi$ actually maps elements of $X_p$ in $X_p$, so that it is well defined. We will denote $(x', y', z') := f(x, y, z)$. Then

- If $(x, y, z) \in A$, so that $f(x, y, z) \in C$, then

$$\begin{aligned} f^2(x, y, z) &= f(x + 2z, z, y - x - z) = (x' - 2y', x' - y' + z', y') \\ &= (x + 2z - 2z, x + 2z - z + y - x - z, z) = (x, y, z). \end{aligned}$$

- If $(x, y, z) \in C$, so that $f(x, y, z) \in A$, then

$$\begin{aligned} f^2(x, y, z) &= f(x - 2y, x - y + z, y) = (x' + 2z', z', y' - x' - z') \\ &= (x - 2y + 2y, y, x - y + z - (x - 2y) - y) = (x, y, z). \end{aligned}$$

- If $(x,y,z) \in B$, so that $f(x,y,z) \in B$, then

$$\begin{aligned} f^2(x,y,z) &= f(2y-x, y, x-y+z) = (2y'-x', y', x'-y'+z') \\ &= (2y-(2y-x), y, 2y-x-y+x-y+z) = (x,y,z). \end{aligned}$$

(e) First, for each $(x,y,z)$ in $A$, $B$ or $C$, we prove that the image of $(x,y,z)$ is in $X_p$ and precisely in the subset prescribed in the exercise. Again, for $(x,y,z) \in X_p$, we use the notation $(x',y',z') = f(x,y,z)$.

- If $(x,y,z) \in A$, then $x+2z$, $z$ and $y-z-x$ are all non-negative and

$$x'^2 + 4y'z' = (x+2z)^2 + 4z(y-x-z) = x^2 + 4yz = p,$$

so that $f(x,y,z) \in X_p$. Moreover,

$$x' - 2y' = x > 0$$

This means that $f(A) \subseteq C$.

- If $(x,y,z) \in B$, then $2y-x, y$ and $x-y+z$ are all non-negative and

$$\begin{aligned} x'^2 + 4y'z' = (2y-x)^2 + 4y(x-y+z) = x^2 + 4yz = p \\ y' - z' = 2y - x - z < 2y - x = x' < 2y = 2y', \end{aligned}$$

so that $f(x,y,z) \in B$.

- If $(x,y,z) \in C$, then $x-y+z > x > x-2y > 0$, $y > 0$ and

$$\begin{aligned} x'^2 + 4y'z' = (x-2y)^2 + 4(x-y+z)y = x^2 + 4yz = p \\ x' = x - 2y < (x-y+z) - y = y' - z' \end{aligned}$$

since $z > 0$, so that $f(x,y,z) \in A$.

*Notice that assuming that $f$ is an involution, then the fact that $f$ switches $A$ and $C$ already immediately implies that $f(B) \subseteq B$, because $b = f(f(b))$ cannot be in $B$ if $f(b) \notin B$. However, since in part (d) we used all the three inclusions that we have just proved in order to show that $f$ is an involution, we cannot skip the proof that $f(B) \subseteq B$, else there would be a circular argument.*

Suppose that $(x,y,z) \in X_p$ is a fixed point. Then it must belong to $B$ but what we have just proved. The map $f$ on $B$ extends to the $\mathbb{Q}$-linear map $\hat{f} : \mathbb{Q}^3 \longrightarrow \mathbb{Q}^3$ given by the matrix

$$M = \begin{pmatrix} -1 & 2 & 0 \\ 0 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix}$$

In order to find fixed points, we look at the eigenvectors associated to 1, that is, at the subspace of $\mathbb{Q}^3$ described by the matrix

$$M - I = \begin{pmatrix} -2 & 2 & 0 \\ 0 & 0 & 0 \\ 1 & -1 & 0 \end{pmatrix}.$$

Hence the fixed points of $X_p$ are all those of the form $(x, x, z) \in \mathbb{Z}^3_{\geqslant 0}$ which satisfy $x^2 + 4xz = p$ and $x - z < x < 2x$. The inequality is always true because $x, z \in \mathbb{Z}$ already remarked above, whereas the equality

$$p = x^2 + 4xz = x(x + 4z) \tag{4}$$

implies that $x = 1$ and $x+4z = p$, since $x < x+4z$ are two distinct factors of $p$. This is true for $x = 1$ and for a unique value $z = z_0$ for which $p = 1 + 4z_0$ (which is the case by hypothesis on $p$). The unique fixed point of $f$ is then $(1, 1, z_0)$. Notice that it is in $B$.

(f) Parts (b), (c) and (e) together imply that $|X_p|$ is odd. Then part (a) implies that $g$ has a fixed point $(x_0, y_0, z_0) \in X_p$, which means $y_0 = z_0$. Hence there exist $x_0, z_0 \in \mathbb{Z}_{\geqslant 0}$ such that $x_0^2 + 4z_0^2 = p$. Let $x = x_0$ and $y = 2y_0$. Then $x^2 + y^2 = p$ as desired.

(g) If $p = x^2 + y^2$ is odd, then exactly one out of $x$ and $y$ is odd. WLOG suppose it is $x$ and write $x = 2k+1$. Then $x^2 = 4k^2+1$. On the other hand, $y^2 = 4\ell$ for some $\ell \in \mathbb{Z}$ since $2 \mid y$. Then $p = 4k^2+1+e\ell$, which means that $p \equiv 1 \pmod 4$.

4. Let $S$ be a set. A *well-order* on $S$ is a total order on $S$ such that every non-empty subset $S$ has a minimal element. For example, the natural order in $\mathbb{N}$ is a well-order.

   (a) Define a well-order on $\mathbb{Z}$.

   (b) Define a well-order on $\mathbb{Q}$.

   (c) Using Zorn's lemma, prove that every set $S$ admits a well-order. [*Hint:* Consider the partially ordered set

   $$\mathcal{S} := \{(A, R) : A \subseteq S,\ R \text{ is a well-order on } A\}$$

   endowed with the partial order defined by

   $$(A, R) \leqslant (A', R') \overset{\text{def.}}{\iff} \left( \begin{array}{c} A \subseteq A'; \forall x, y \in A, xRy \iff xR'y \\ \text{and } \forall a \in A, \forall a' \in A', a'R'a \implies a' \in A \end{array} \right).$$

   Check that $(\mathcal{S}, \leqslant)$ satisfies the hypotheses of Zorn's lemma and get a maximal element $(M, R_0)$. Prove that $M = S$.]

*Solution*: For every bijection $\varphi : S \xrightarrow{\sim} \mathbb{N}$, one can define a total order $\leqslant$ on $S$ via $s \leqslant t \overset{\text{def.}}{\iff} \varphi(s) \leqslant \varphi(t)$.

(a) Consider the bijection $\varphi : \mathbb{Z} \longrightarrow \mathbb{N}$ sending $0 < k \mapsto 2k - 1$ and $0 \geqslant k \mapsto 2k$. This is easily seen to be a bijection and it induces the following well-order on $\mathbb{Z}$:

$$0 \leqslant 1 \leqslant -1 \leqslant 2 \leqslant -2 \leqslant 3 \leqslant -3 \leqslant \dots$$

(b) One can construct a bijection $\psi : \mathbb{Z} \longrightarrow \mathbb{Q}$ as follows:

- $\psi(0) = 0$;
- $\psi(-n) = -\psi(n)$ for each $n$;
- write, for $k \in \mathbb{Z}_{>0}$,

$$F_k := \left\{ \frac{a}{b} \in \mathbb{Q} : \gcd(a, b) = 1,\ a + b = k + 1 \right\}$$

  and denote $f_k := |F_k| < k + 1$. Then the values of $\psi(n)$ for $n > 0$ range, in the order, on the sets $F_1 = \{1\}, F_2 = \{2, 1/2\}, F_3, \dots$ starting, in each $F_k$, with the fraction of highest denominator. This means that $\psi(n) \in F_k$ if and only if $\sum_{j=1}^{k-1} f_j < n \leqslant \sum_{j=1}^{k} f_j$, and in this case $\psi(n)$ is equal to the $(n - \sum_{j=1}^{k-1} f_j)$-th element in $F_k$, the elements in $F_k$ being ordered with decreasing denominators.

The map $\psi$ is a bijection because the $F_j$'s form a partition of $\mathbb{Q}_{>0}$. Considering $\varphi$ as in the previous part, the bijection $\varphi \circ \psi^{-1} : \mathbb{Q} \longrightarrow \mathbb{N}$ induces the following well-order on $\mathbb{Q}$:

$$0 \leqslant 1 \leqslant -1 \leqslant \frac{1}{2} \leqslant -\frac{1}{2} \leqslant 2 \leqslant -2 \leqslant \frac{1}{3} \leqslant -\frac{1}{3} \leqslant 3 \leqslant -3 \leqslant \frac{1}{4} \leqslant -\frac{1}{4} \leqslant \frac{2}{3} \leqslant \dots$$

(c) We follow the hint. We first notice that $\leqslant$ defines a partial order on $\mathcal{S}$: reflexivity is clear, antisymmetry descends from the same property on sets and transitivity is immediate by definition.

Now we check that $(\mathcal{S}, \leqslant)$ satisfies the hypothesis of Zorn's lemma:

- $\mathcal{S} \neq \varnothing$, as it contains $(\varnothing, \varnothing)$.
- For every chain $(A_i, R_i)_{i \in I} \subseteq \mathcal{S}$, consider $A_0 = \bigcup_{i \in I} A_i$. Define a relation $R_0$ on $A_0$ as follows: for $a_1 \in A_{i_1}$ and $a_2 \in A_{i_2}$, let $j = \max\{i_1, i_2\}$ (the total order on $i$ being induced by $(A_i, R_i)_{i \in I}$ being a chain), so that $a_1, a_2 \in A_j$, and we set $a_1 R_0 a_2$ if and only if $a_1 R_j a_2$. This relation is well defined: if it is also the case that $a_1 \in A_{i'_1}$ and $a_2 \in A_{i'_2}$ with $j' = \max\{i'_1, i'_2\}$, let $J := \max\{j, j'\}$; then

$$a_1 R_j a_2 \iff a_1 R_J a_2 \iff a_1 R_{j'} a_2,$$

because the $R_J$ is an extension of both $R_j$ and $R_{j'}$ by definition of the partial order $\leqslant$ on $\mathcal{S}$.

All the axioms for $R_0$ being a total order are satisfied because each $R_i$ is a well-order. For example, totality is proven by noticing that for each $a_1, a_2 \in A_0$ there exist $i_1, i_2 \in I$ such that $a_\lambda \in A_{i_\lambda}$ and for $j = \max\{a_1, a_2\}$ one obtains that $a_1, a_2 \in A_j$, so that either $a_1 R_j a_2$ (and then $a_1 R_0 a_2$) or $a_2 R_j a_1$ (and then $a_2 R_0 a_1$), as $R_j$ is a total order.

Consider now a non-empty subset $A_{00}$ of $A_0$. Let $i \in I$ be such that $A_{00} \cap A_i \neq \varnothing$. Then the set $A_{00} \cap A_i \subseteq A_i$ has a minimum $a_{0i}$ with respect to $R_i$. Let $a_{00} \in A_{00}$ and let $j \in I$ be such that $a_0 0 \in A_j$. We want to show that $a_{0i} R_0 a_{00}$, so that we can prove that $a_{0i}$ is minimal element of $A_{00}$. In order to show that $a_{0i} R_0 a_{00}$ it is enough to check that $a_{0i} R_j a_{00}$. This is clearly the case if $A_j \subseteq A_i$, so assume that $(A_i, R_i) \leqslant (A_j, R_j)$ strictly, so that $a_{00} \in A_j \smallsetminus A_i$. Suppose that $a_{00} R_j a_{0i}$. Then, by definition of $\leqslant$ on $\mathcal{S}$, we get $a_0 0 \in A_i$, a contradiction, so that $\neg a_{00} R_j a_{0i}$ and by totality of $R_j$ we have $a_{0i} R_j a_{00}$. This allows us to deduce that $(A_0, R_0) \in \mathcal{S}$.

Finally, $(A_i, R_i) \leqslant (A_0, R_0)$ for each $i \in I$ because $A_i \subseteq A_0$ by definition of $R_0$.

By Zorn's lemma, we obtain a maximal element $(M, R_0)$ of $(\mathcal{S}, \leqslant)$ and we now prove that $M = S$. Suppose by contradiction that $S \smallsetminus M \neq \varnothing$. Let $s \in S \smallsetminus M$. On the set $M \cup \{s\}$, define the order for which $t_1 R' t_2$ if and only if $t_1 = s$ or $t_1, t_2 \in M$ and $t_1 R_0 t_2$. Then $R'$ is a well-order on $M \cup \{s\}$. Indeed, it is a total order because the freshly added element can be compared with all elements in $M \cup \{s\}$ and, moreover, every subset of $M \cup \{s\}$ has a minimum, because either it is a subset of the well-ordered set $(M, R_0)$ or it contains $s$ which satisfies $s R' t$ for each $t \in M \cup \{s\}$.