Revision

CS1231S Discrete Structures

Wong Tin Lok

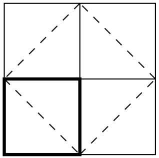
National University of Singapore

13 November 2020

Afternoon mass consultation sessions

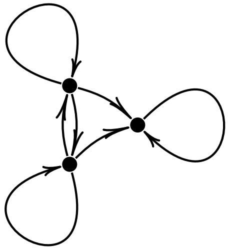
Wednesday 18 Nov, Friday 20 Nov, Tuesday 24 Nov 16:00–17:30

Draw a square whose area is double that of this square.



I should not only speak the truth, but I should make use of premisses which the person interrogated would be willing to admit. Socrates in Plato's *Meno*

What we saw after the Recess Week

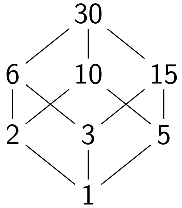


Basic number theory

- divisibility and division (quotient and remainder)
- primes (infinitude of primes)
- base-b representation
- greatest common divisors (the Euclidean Algorithm, Bézout's Lemma)
- prime factorizations (the Fundamental Theorem of Arithmetic)
- modular arithmetic (congruence, multiplicative inverses)

Relations

- reflexivity, symmetry, transitivity, antisymmetry
- equivalence relations (equivalence classes), partitions
- partial orders (Hasse diagrams, smallest/largest and minimal/maximal elements, total orders, linearization)



Do not forget what we saw before the mid-term test!

Assignment 2 Question 5

Let $\mathscr{C}$ be a partition of A. Show that there exist a set B and a surjection $f\colon A \to B$ such that

$$\mathscr{C} = \big\{\{x \in A : f(x) = y\} : y \in B\big\}.$$

- We want to prove a statement of the form $\forall \mathscr{C}\ \exists B\ \exists f\colon A \to B\ \ldots$.
- So given *any* $\mathscr{C}$, we have to produce B and f with the required properties.
- We cannot control what $\mathscr{C}$ is, but we can (and should) control what B and f are.
- Why do many split into the cases "A is empty" and "A is nonempty"?
- What do you mean by "So B exists"?
- Writing $\mathscr{C} = \{S_1, S_2, \ldots, S_n\}$ implies $\mathscr{C}$ is finite. Not all partitions are finite.
- Writing $\mathscr{C} = \{S_i : i \in \mathbb{Z}_{\geqslant 1}\}$ implies $\mathscr{C}$ is countable. Not all partitions are countable.

- My choice: let $B = \mathscr{C}$ and $f(x) = S$ if and only if $x \in S$ for all $x \in A$ and $S \in \mathscr{C}$.
- Axiom of Choice: choose an element x_S from each $S \in \mathscr{C}$; let $B = \{x_S : S \in \mathscr{C}\}$ and $f(x) = x_S$ if and only if $x \in S$ for all $x \in A$ and $S \in \mathscr{C}$.

2019/20 Semester 1 exam

16 (c) Find a positive integer that has exactly 5 positive divisors.

(d) Let $A = \{0, 1, 2, \ldots, 11\}$. For each $a \in A$, define $m_a\colon A \to A$ by $m_a(x) = ax \mathbin{\underline{\mathrm{mod}}} 12$. Find an $a \in A \setminus \{1\}$ such that m_a is bijective.

17 Let P be a partial order on a nonempty set A. Let R be another relation on A, and suppose $R \subseteq P$. Let $\tilde{R}$ be the reflexive closure of R and let T be the transitive closure of $\tilde{R}$. Prove that:

(a) T is a partial order on A.

(b) If T' is another partial order on A such that $R \subseteq T'$, then $T \subseteq T'$.

Recall from Tutorial 8 [of that semester] that the reflexive closure of a relation is the smallest reflexive relation on the same set that contains this relation as a subset. Similarly, the transitive closure of a relation is the smallest transitive relation on the same set that contains this relation as a subset.

20 Let $n \in \mathbb{Z}^+$ with $n \geqslant 3$, and let $A = \{0, 1, \ldots, n-1\}$. Prove that there exists an $m \in A$ such that $m \not\equiv a^2 \pmod{n}$ for any $a \in \mathbb{Z}$.

2019/20 Semester 1 exam Q16(c)

Find a positive integer that has exactly 5 positive divisors.

Solution

- Let $p_0^{m_0} p_1^{m_1} \dots p_\ell^{m_\ell}$ be the prime factorization of an integer n, where $p_0, p_1, \dots, p_\ell$ are distinct primes and $m_0, m_1, \dots, m_\ell \in \mathbb{Z}^+$.
- Then the positive divisors of n are precisely those integers of the form $p_0^{k_0} p_1^{k_1} \dots p_\ell^{k_\ell}$, where each $k_i \in \{0, 1, \dots, m_i\}$.
- There are $m_0 + 1$ choices for k_0, $m_1 + 1$ choices for k_1, $\dots$, $m_\ell + 1$ choices for k_ℓ.
- So altogether there are exactly $(m_0 + 1)(m_1 + 1) \cdots (m_\ell + 1)$ positive divisors of n.
- As each $m_i \geqslant 1$, we know $m_i + 1 \geqslant 2$.
- So
$$\begin{aligned} & n \text{ has exactly 5 positive divisors} \\ \Leftrightarrow \quad & \ell = 0 \text{ and } m_0 = 5 - 1 = 4 \qquad \text{as 5 is prime;} \\ \Leftrightarrow \quad & n = p_0^4. \end{aligned}$$
- Hence we can take $n = 2^4 = 16$, or $n = 3^4 = 81$, or $n = 5^4 = 625$, or $\dots$.

2019/20 Semester 1 exam Q16(d)

Let $A = \{0, 1, 2, \dots, 11\}$. For each $a \in A$, define $m_a : A \to A$ by $m_a(x) = ax \,\underline{\text{mod}}\, 12$.
Find an $a \in A \setminus \{1\}$ such that m_a is bijective.

Solution

- Let $a \in A$ such that $\gcd(a, 12) = 1$. This means $a \in \{5, 7, 11\}$.
- We show that m_a is injective.

1. Let $x, y \in A$ such that $m_a(x) = m_a(y)$, i.e., $(ax \,\underline{\text{mod}}\, 12) = (ay \,\underline{\text{mod}}\, 12)$.
2. Then $ax \equiv ay \pmod{12}$ by the definition of congruence.
3. As $\gcd(a, 12) = 1$, the number a has a multiplicative inverse modulo 12, say b.
4. Multiplying b to both sides of the congruence in line 2 gives $bax \equiv bay \pmod{12}$.
5. As b is a multiplicative inverse of a modulo 12, this implies $x \equiv y \pmod{12}$.
6. The definition of congruence then tells us $(x \,\underline{\text{mod}}\, 12) = (y \,\underline{\text{mod}}\, 12)$.
7. As $x, y \in A = \{0, 1, \dots, 11\}$, we know $(x \,\underline{\text{mod}}\, 12) = x$ and $(y \,\underline{\text{mod}}\, 12) = y$.
8. Hence $x = y$.

- So A has the same number of elements as the range of m_a, which is a subset of A.
- As A is finite, this implies the A equals range of m_a, and thus m_a is bijective.

2019/20 Semester 1 exam Q17(a)

Let P be a partial order on a nonempty set A. Let R be another relation on A, and suppose $R \subseteq P$. Let $\tilde{R}$ be the reflexive closure of R and let T be the transitive closure of $\tilde{R}$. Prove that T is a partial order on A.

Recall from Tutorial 8 [of that semester] that the *reflexive closure* of a relation is the smallest reflexive relation on the same set that contains this relation as a subset. Similarly, the *transitive closure* of a relation is the smallest transitive relation on the same set that contains this relation as a subset.

Proof

1. (Reflexivity) If $x \in A$, then $(x, x) \in \tilde{R}$ as $\tilde{R}$ is reflexive, and so $(x, x) \in T$ as $\tilde{R} \subseteq T$.
2. (Transitivity) T is transitive because it is a transitive closure.
3. (Antisymmetry)
   - 3.1. Note that $P \supseteq R$ and P is reflexive. So $P \supseteq \tilde{R}$ by the minimality of $\tilde{R}$.
   - 3.2. Note that $P \supseteq \tilde{R}$ and P is transitive. So $P \supseteq T$ by the minimality of T.
   - 3.3. If $x, y \in A$ such that $(x, y), (y, x) \in T$, then $(x, y), (y, x) \in P$ as $T \subseteq P$, and so $x = y$ by the antisymmetry of P. $\square$

2019/20 Semester 1 exam Q17(b)

Let P be a partial order on a nonempty set A. Let R be another relation on A, and suppose $R \subseteq P$. Let $\tilde{R}$ be the reflexive closure of R and let T be the transitive closure of $\tilde{R}$. Prove that if T' is another partial order on A such that $R \subseteq T'$, then $T \subseteq T'$.

Recall from Tutorial 8 [of that semester] that the *reflexive closure* of a relation is the smallest reflexive relation on the same set that contains this relation as a subset. Similarly, the *transitive closure* of a relation is the smallest transitive relation on the same set that contains this relation as a subset.

Proof

1. Let T' be a partial order on A such that $R \subseteq T'$.
2. Note that $T' \supseteq R$ and T' is reflexive.
3. So $T' \supseteq \tilde{R}$ by the minimality of $\tilde{R}$.
4. Note that $T' \supseteq \tilde{R}$ and T' is transitive.
5. So $T' \supseteq T$ by the minimality of T. $\square$

2019/20 Semester 1 exam Q20

Let $n \in \mathbb{Z}^+$ with $n \geqslant 3$, and let $A = \{0, 1, \ldots, n-1\}$. Prove that there exists an $m \in A$ such that $m \not\equiv a^2 \pmod{n}$ for any $a \in \mathbb{Z}$.

1. Define $f\colon A \to A$ by setting $f(b) = (b^2 \,\underline{\text{mod}}\, n)$ for all $b \in A$.
2. We show that f is not injective.
   - 2.1. Note that $(n-1)^2 = n^2 - 2n + 1 \equiv 1 \pmod{n}$.
   - 2.2. So the definition of congruence implies $((n-1) \,\underline{\text{mod}}\, n) = (1 \,\underline{\text{mod}}\, n)$.
   - 2.3. Thus $f(n-1) = f(1)$. But $n - 1 \neq 1$ as $n \geqslant 3$.
3. As A is finite and $f\colon A \to A$, we deduce that f is not surjective.
4. Pick $m \in A$ such that $m \neq f(b)$ for all $b \in A$.
5.
   - 5.1. Take any $a \in \mathbb{Z}$.
   - 5.2. Let $b = (a \,\underline{\text{mod}}\, n)$, so that $b \in A$, and thus $m \neq f(b)$ by line 4.
   - 5.3. Then the definition of f implies $m \neq (b^2 \,\underline{\text{mod}}\, n)$.
   - 5.4. As $m, b \in \{0, 1, \ldots, n-1\}$, we know $(m \,\underline{\text{mod}}\, n) = m$ and $(b \,\underline{\text{mod}}\, n) = b$.
   - 5.5. So $(m \,\underline{\text{mod}}\, n) \neq (b^2 \,\underline{\text{mod}}\, n)$ and $(b \,\underline{\text{mod}}\, n) = (a \,\underline{\text{mod}}\, n)$ by lines 5.2 and 5.3.
   - 5.6. Thus $m \not\equiv b^2 \pmod{n}$ and $b \equiv a \pmod{n}$, implying $m \not\equiv a^2 \pmod{n}$. $\square$

2019/20 Semester 1 exam Q6

Which of the following is a partition of the set P of all prime numbers?

A. $\big\{\{p \in P : p \equiv a \pmod 4\} : a \in \{0, 1, 2, 3\}\big\}$.

B. $\big\{\{p \in P : p \equiv a \pmod 4\} : a \in \{1, 2, 3\}\big\}$.

C. $\big\{\{p \in P : p \equiv a \pmod 4\} : a \in \{0, 1, 3\}\big\}$.

D. $\big\{\{p \in P : p \equiv a \pmod 4\} : a \in \{1, 3\}\big\}$.

E. None of the above.

Solution

- $\{p \in P : p \equiv 0 \pmod 4\} = \varnothing$ because if $p \equiv 0 \pmod 4$, then $1, 2, 4$ are divisors of p, and so p cannot be prime.
- $\{p \in P : p \equiv 1 \pmod 4\} = \{5, \dots\}$.
- $\{p \in P : p \equiv 2 \pmod 4\} = \{2\}$.
- $\{p \in P : p \equiv 3 \pmod 4\} = \{3, \dots\}$.
- So option B is the correct answer.