CSCA67 Final Review

① if $x>a>0$, then $x^2>a^2$

proof: $x>a$

$\left.\begin{array}{l} xa>a^2 \\ x^2>ax \end{array}\right\}$ since $x>a>0$

$\therefore x^2>xa>a^2$

$\therefore x^2>a^2$ QED

$a \bmod n = b$ means that $a \div n$ has a remainder b

$a \equiv_n b$ means that $a \bmod n = b \bmod n$

n divide $(a-b)$: $n \mid (a-b)$

: concepts

: keys

: questions

② Prove $\sqrt{2}$ is irrational

contradiction: $\sqrt{2}$ is rational

$\sqrt{2}=\frac{p}{q} \Leftrightarrow \sqrt{2}q=p$

$2q^2 \Leftrightarrow p^2$

$q=x_1 \cdot x_2 \cdot x_3 \cdot x_4 \cdots x_n$

$p=y_1 \cdot y_2 \cdot y_3 \cdots y_k$

$2q^2=\underbrace{(x_1 \cdot x_2 \cdot x_3 \cdot x_4 \cdots x_n)(x_1 \cdot x_2 \cdot x_3 \cdot x_4 \cdots x_n) \cdot 2}_{2n+1 \text{ prime}}$

$p^2=\underbrace{(y_1 \cdot y_2 \cdot y_3 \cdots y_k)(y_1 \cdot y_2 \cdot y_3 \cdots y_k)}_{2k}$

odd ≠ even

contradiction ✓

QED.

③ prove infinite prime number

contradiction: finite prime number

$P_1, P_2, P_3 \dots P_n$

consider $x=(P_1 \cdot P_2 \cdot P_3 \cdots P_n)+1$

none of our prime number divides x

$\therefore x$ has a unique prime factor

$\therefore$ either x is prime or $\exists$ other prime factor that not in the list we listed. Contradiction ✓

QED.

$S \to T \Leftrightarrow \neg S \vee T$

$S \to T \Leftrightarrow \neg T \to \neg$

④ prove if 2^n-1 is prime than n is prime

contrapositive: $\forall n \in N^+$, n not prime $\to 2^n-1$ not prime

Let $n=x \cdot y$

$x \geq 2, y \geq 2$

$2^n-1=2^{x \cdot y}-1=(2^x)^y-1$

$(2^x)^y-1=\underbrace{(2^x-1)}_{\geq 3}[\underbrace{(2^x)^{y-1}}_{\geq 4}+(2^x)^{y-2}+(2^x)^{y-3}+\dots+\underbrace{2^x}_{\geq 5}+1)$

$(2^x)^y-1 \geq 4$ QED.

$n=x \cdot y$

$x \geq 2$

$y \geq 2$

$(2^x)^y-1=\underbrace{(2^x-1)}_{\geq 3}[(2^x)^{y-1}+(2^x)^{y-2}+\dots+\underbrace{2^x}_{\geq 5}+1)$

PHP: if n item are put into m containers, with $n>m$, then at least one container must contain more than one item.

⑤ Show that given a set of n positive integers, $\exists$ a non-empty subset whose sum is divisible by

Let the set be $\{a_1, a_2, a_3, a_4 \cdots a_{n-1}, a_n\}$.

we have $s_1 = a_1$
$s_2 = a_1 + a_2$
$s_3 = a_1 + a_2 + a_3$
$s_i = a_1 + a_2 + \cdots + a_i$
$s_n = a_1 + a_2 + \cdots a_n$

case 1: if any s_i is divisible by n, we done

case 2: no s_i divisible by n. so $s_i = nq + r_i$ $1 \le r_i \le n$

there are $n-1$ possible value for r_i

we have n sum, $(n-1)$ possible value for r..

By PHP, two of the sum have the same remainder.

$$\left.\begin{aligned} S_m &= a_1 + a_2 + a_3 + \cdots + a_m = nq_m + r \\ S_n &= a_1 + a_2 + \cdots + a_n = nq_n + r \end{aligned}\right\} r = r$$

$S_m - S_n = n(q_m - q_n)$ which is divisible by n.

QED

⑥ chocolate (Strong Induction)

$S(n)$: $n \ge 1$, break n square require $n-1$

Base Case: $S(1)$, 1×1 requires $1\times1-1=0$ ✓

Inductive Hypothesis: Let $n \in \mathbb{N}$, suppose that $S(n)$ holds with less than n.

$\forall k \in \mathbb{N}$, $0 < k < n$, $S(k)$. (not a single k but for all k under the restriction)

Inductive Step: prove $\forall k \in \mathbb{N}, (0 < k < n \wedge S(k)) \to S(n)$

assume there is a single and we break it into a squares and b square.

$0 < a < n$ and $0 < b < n$ (by IH)

a requires $a-1$
b requires $b-1$

total: $(a-1)+(b-1)+1 = a+b-1$
$= n-1$

$\therefore$ # of total break $n-1$

$S(n)$ holds.

Sum rule: $P(E \text{ or } F) = P(E) + P(F) - \underbrace{P(E \text{ and } F)}_{\text{overlap.}}$

$P(E|F)$: the probability of E depend on previous F