CS201-Midterm

12011517_李子南

Q1.

(1)Incorrect

$(\neg p \wedge (p \rightarrow q)) \rightarrow \neg q$

$\equiv \neg(\neg p \wedge (\neg p \vee q)) \vee \neg q$

$\equiv p \vee (p \wedge \neg q) \vee \neg q$

$\equiv p \vee \neg q$

Therefore when p is False and q is True, the statement is false.

(2)Correct

$(p \vee q) \rightarrow r \equiv (\neg p \wedge \neg q) \vee r$

$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (\neg p \vee r) \wedge (\neg q \vee r) \equiv (\neg p \wedge \neg q) \vee r$

Therefore they are equivalent.

(3)Correct

For any y we have $x = \frac{1}{y}$ that $y * \frac{1}{y} = 1$

(4)Correct

There exist $1^2 + 2^2 = 5$

Q2.

(1)It's invalid. It does not follow modus ponens.

Set finish homework as p, can answer this question as q

Then premise1: $\neg p \rightarrow \neg q$

Premise 2: p

When q is false the premises above still holds. Therefore it's invalid.

(2)It's invalid. It doesn't follows modus ponens or modus tollens.

Set all students in this class has submitted their homework as p, all students can get 100 in the final exam as q

Then premise1: $p \rightarrow q$

Premise2: $\neg p$

When q is true the premises above still holds. Therefore it's invalid.

Q3.

$(\neg r \vee (p \wedge \neg q)) \rightarrow (r \wedge p \wedge \neg q)$

$\equiv (r \wedge (\neg p \vee q)) \vee (r \wedge p \wedge \neg q)$

$\equiv r \wedge (\neg p \vee q \vee (p \wedge \neg q))$

$\equiv r$

$(\neg r \vee (p \wedge \neg q)) \rightarrow (r \wedge p \wedge \neg q) \rightarrow (r \vee s)$

$\equiv \neg r \vee r \vee s$

$\equiv True$

Therefore $(\neg r \vee (p \wedge \neg q)) \rightarrow (r \wedge p \wedge \neg q)$ implies $r \vee s$

Q4.

(1)False

Assume $A = \{a, b\}, B = \{1, 2\}$

$A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$

$B \times A = \{(1, a), (1, b), (2, a), (2, b)\}$

$A \times B \neq B \times A$

Therefore $P(A \times B) \neq P(B \times A)$

(2)True

$(A \oplus B) = A \cup B - A \cap B$

$(A \oplus B) \oplus B = (A \cup B - A \cap B) \cup B - (A \cup B - A \cap B) \cap B$

$(A \cup B - A \cap B) \cup B = A \cup B$

$(A \cup B - A \cap B) \cap B = (B - A \cap B)$

$(A \oplus B) \oplus B = A \cup B - (B - A \cap B) = A$

(3)False

Assume $S, T \in Z\ S = \{1\}, T = \{2\}, f : \{1, 2\} \rightarrow \{0\}$

Then $f(S \cap T) = f(\emptyset) = \emptyset,\ f(S) \cap f(T) = \{0\}$

Therefore$f(S \cap T) \neq f(S) \cap f(T)$ the statement is false.

(4)True

Because function f have inverse function f^{-1}

Therefore f is bijective

Thus for $p, q \in B((f^{-1}(p) = f^{-1}(q)) \rightarrow (p = q))$

and $\forall m \in A \exists n \in B(f^{-1}(n) = m)$

Therefore $\forall x \in (S \cap T)((f^{-1}(x) \subseteq f^{-1}(S)) \wedge (f^{-1}(x) \subseteq f^{-1}(T)))$

Thus $f^{-1}(S \cap T) \subseteq f^{-1}(S) \cap f^{-1}(T)$

Therefore $\forall x \in S(f^{-1}(x) \subseteq f^{-1}(S \cap T))$,$\forall x \in T(f^{-1}(x) \subseteq f^{-1}(S \cap T))$

Thus $f^{-1}(S) \cap f^{-1}(T) \subseteq f^{-1}(S \cap T)$

Therefore $f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T)$

Q5.

Assume there exist an infinite set A that $|A| < |Z^+|$

Function $f: Z^+ \to A$

For $n \in Z^+$, m is the n^{th} smallest number in A, hence $f(n) = m$

Because $p, q \in Z^+$, $p \neq q$ leads to $f(p) \neq f(q)$, f is injective.

Therefore $|Z^+| \leq |A|$, exist contradiction

Therefore there does not exist an infinite set A that $|A| < |Z^+|$

Q6.

$(log\, n)^{log\, log\, n},\ log(n^n),\ n^2(log\, n)^{20},\ n^{20},\ 2^n,\ (n!)^{20}$

$log(n^n) = nlog\, n$

$$\lim_{n\to\infty} \frac{nlog\, n}{(log\, n)^{log\, log\, n}} = \lim_{n\to\infty} \frac{n}{(log\, n)^{log\, log\, n-1}} = \infty$$

Therefore there exist c when $n > c$,$k = 1$, $(log\, n)^{log\, log\, n} < klog(n^n)$

$(log\, n)^{log\, log\, n} = O(log(n^n))$

Q7.

According to the text, we have

$x \equiv 1(mod\, 2)$

$x \equiv 0(mod\, 3)$

$x \equiv 1(mod\, 4)$

$x \equiv 4(mod\, 5)$

$x \equiv 3(mod\, 6)$

$x \equiv 0(mod\, 7)$

$x \equiv 1(mod\, 8)$

$x \equiv 0(mod 9)$

We can convert these equations to:

$x \equiv 0(mod\, 3)$

$x \equiv 4(mod\, 5)$

$x \equiv 0(mod\, 7)$

$x \equiv 1(mod\, 8)$

Using Chinese remainder theorem

$m = 840, M_1 = 280, M_2 = 168, M_3 = 120, M_4 = 105$

$M_1 \times 1 \equiv 1(mod\, 3)$

$M_2 \times 2 \equiv 1(mod\, 5)$

$M_3 \times 1 \equiv 1 (mod\, 7)$

$M_4 \times 1 \equiv 1 (mod\, 8)$

$x \equiv 4 \times 168 \times 2 + 1 \times 105 \times 1 = 1449 \equiv 609 (mod\, 840)$

Therefore there are $609 + 840k, k \in N$ People in total.

Q8.

(1)$(33^{15}\ mod\, 32) = (33\ mod\, 32)^{15} = 1$

$(33^{15}\ mod\, 32)^3\ mod\, 15 = 1\ mod\, 15 = 1$

(2)$1638/210 = 7 \ldots\ 168$

$210/168 = 1 \ldots\ 42$

$168/42 = 4$

Therefore $gcd(210, 1638) = 42$

(3)$89 = 2 \times 34 + 21$

$34 = 1 \times 21 + 13$

$21 = 1 \times 13 + 8$

$13 = 1 \times 8 + 5$

$8 = 1 \times 5 + 3$

$5 = 1 \times 3 + 2$

$3 = 2 + 1$

Reversely we can get $1 = 13 \times 89 - 34 \times 34$

$34 * 34x \equiv 34 * 77 (mod\, 89)$

Therefore $x \equiv 37 (mod\, 89)$

(4) According to Fermat's little theorem, we have $3^1 \equiv 1(mod\, 2), 3^4 \equiv 1(mod\, 5)$

Therefore $3^{1000} \equiv 3^{1000\ mod\, 1} \equiv 1(mod\, 2),\ 3^{1000} \equiv 3^{1000\ mod\, 4} \equiv 1(mod\, 5)$

Because $gcd(2, 5) = 1, 3^{1000} \equiv 1(mod\, 2), 3^{1000} \equiv 1(mod\, 5)$

Therefore $3^{1000} \equiv 1(mod\, 10)$

The last decimal digit of 3^{1000} is 1

Q9.

Assume there is a odd factor that $t|m$, then $m = kt$, we have

$2^m + 1 = (2^k + 1)(2^{k(t-1)} - 2^{k(t-2)} +\ \ldots\ - 2^k + 1)$

Because $k > 1, t > 1,$ therefore $2^m + 1$ is not prime and thus a contradiction.

Therefore m does not has any odd factor that is grater than one.

Q10.

$n = 5429 = 89 * 61$

$(89 - 1)(61 - 1) = 5280$

(1)$5280/61 = 86 \ldots\ 34$

$61/34 = 1 \ldots\ 27$

$34/27 = 1 \ldots\ 7$

$27/7 = 3 \ldots\ 6$

$7/6 = 1 \ldots 1$

$gcd(61, 5280) = 1$

$de = 274561 \equiv 1(mod\, 5280)$

This pair is valid

(2)$5280/89 = 59 \ldots\ 29$

$89/29 = 3 \ldots\ 2$

$29/2 = 14 \ldots\ 1$

$gcd(89, 5280) = 1$

$de = 251781 \equiv 3621(mod\, 5280)$

This pair is invalid

(3)$gcd(5280, 30) \neq 1$

This pair is invalid

Q11.

My mom always said life was like a box of chocolates. You never know what you're gonna get.

First I count the frequency each letter appears:

a 9

b

c 7

d

e 2

f

g 2

h 2

i 8

j 1

k

l 4

m 2

n 1

o 4

p 2

q 3

r 2

s 2

t 1

u 4

v 4

w 3

x 1

y 4

z 3

Then I notice the string "yae'pc", this abbreviation is likely to be "you're".And character 'a' appears most often. Therefore I suppose $y \to y, a \to o, e \to u, p \to r, c \to e$

A single 'i' appears in the middle of the sentence, and i appears 8 times in total, thus I guess

$i \to a$. The first two words are "_y _o_", I tried to fill the blank with P,B and M, it only make sense when $q \to m$

After that, word "vcjcp" become "_e_er", it's easy to get "never", we have $v \to n$, $j \to v$

Then "ah" became "o_", it's only make sence when $h \to f$

Because character 'u' mostly appear in the end of the word, I guess 'u' represents consonant 's', that is $u \to s$

Therefore I can tell "iloiyu" is "always", $o \to w$,$l \to l$, "oiu" is "was", "gvao" is "know"

Then I guess "lwhc" and "lwgc" is "life" and "like"

Because *Forrest Gump* is one of my favorites movies, so I spell the complete sentence easily.

Afterall I found that if we set a as 0, we can solve linear congruence equations

$2x + b \equiv 4(mod\ 26)$, $0x + b \equiv 14(mod\ 26)$

We can get $f(x) = (8x + 14)\ mod\ 26$