CSC165H1: Problem Set 1

Due Wednesday October 4 before 10pm

CSC165H1
Title: Mathematical Expression and Reasoning for Computer Science
Instructor: Danny Heap

Q1

(a)

p	q	R	$(p \lor q) \Longrightarrow r$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	T	T
T	T	F	F
T	F	F	F
F	T	F	F
F	F	F	T

(b)

$\neg(p \lor q) \lor r$

$(\neg p \land \neg q) \lor r$

Q2

(a)

$\forall m, n \in \mathbb{N}, m \equiv 5(\mathrm{mod}7) \land n \equiv 2(\mathrm{mod}7) \Longrightarrow mn \equiv 3(\mathrm{mod}7)$

Let $m, n \in \mathbb{N}$

Assume $\exists k_1, k_2 \in \mathbb{Z}$ s.t. $m - 5 = 7k_1, n - 2 = 7k_2$

Let $k_3 \in \mathbb{Z}$ Let $k_3 = 7k_1k_2 + 2k_1 + 5k_2 + 1$

$$7k_3 = 49k_1k_2 + 14k_1 + 35k_2 + 7$$
$$= (7k_1 + 5)(7k_2 + 2) - 3$$
$$= mn - 3 \quad \blacksquare$$

(b)

$\forall m, n \in \mathbb{N}, mn \equiv 3(\mathrm{mod}7) \Longrightarrow m \equiv 5(\mathrm{mod}7) \land n \equiv 2(\mathrm{mod}7)$

Proof: Let $m, n \in \mathbb{N}$

Let m = 2, n = 5

mn - 3 = 7

7 | 7

m - 5 = -3

$7 \nmid -3$

n - 2 = 3

$7 \nmid 3$ ■

Q3

(a)

Proof: Let f be a function that evaluates how many people each person shook hands with

Let the set of people at the party as the domain

Let the number of people each person shook hands with as the range

We know the pigeonhole principle shows that

$\forall f \in F, \mathrm{OneToOne}(f) \Longrightarrow |D| \leq |R|$

If n $n \geq 2 \in \mathbb{Z}$ people go to the party, then the smallest number of people each person shook hands with is 0 and the greatest number is n - 1

Which means that $|D| \geq |R|$

Let $|D| > |R|$

Then according the pigeonhole principle we can get $\neg\mathrm{OneToOne}(f)$

Which means that

$\exists x, y \in D, x \neq y \wedge f(x) = f(y), \text{where } f: D \mapsto R, |D|, |R| \in \mathbb{N}^{+}$

So far we have proved that if $n \geq 2$people go to the same party, there are at least 2 people who shook hands with the same number of other people ■

Q4

(a)

Proof: Let a, p $\in \mathbb{R}$ with p prime and gcd(a, p) = 1

Let T = {1, …, p - 1}

Let n $\in$ T

We know that p is a prime

Which means $\exists d \in \mathbb{Z}\ \mathrm{s.t.}\ d|p \Rightarrow d = p \vee d = 1$

Because gcd(a, p) = 1

We know that $p \nmid a$

Case1: If n = 1

$r_p(an) = r_p(a)$

According to theorem 2.1 on textbook

$\forall x, d \in \mathbb{Z}, \exists q, r \in \mathbb{Z}\ \mathrm{s.t.}\ x = qd + r \wedge 0 \leq r < x$

We can conclude that $0 \leq r_p(a) < p$

Because $p \nmid a$

Then $0 < r_p(a) < p$

Which means $\{r_p(an) | n \in T\} \subseteq T$

Case2: If n $\in$ [2, p – 1]

Since $\exists d \in \mathbb{Z}\ \mathrm{s.t.}\ d|p \Rightarrow d = p \vee d = 1$

We know that $p \nmid n$

Which means gcd(p, n) = 1

Then $\exists s_1, t_1 \in \mathbb{Z}\ \mathrm{s.t.}\ s_1p + t_1n = 1$

Similarly $\exists s_2, t_2 \in \mathbb{Z}\ \mathrm{s.t.}\ s_2p + t_2a = 1$

WTS $\exists s_3, t_3 \in \mathbb{Z}\ \mathrm{s.t.}\ s_3p + t_3an = 1$

Let $s_3 = s_1s_2 + t_1s_2p + t_2s_1a$

Let $t_3 = t_1 t_2$

Then $s_3 p + t_3 an$

$= (s_1 s_2 + t_1 s_2 p + t_2 s_1 a)p + t_1 t_2 an$

$= (s_1 p + t_1 n) + (s_2 p + t_2 a)$

$= 1$

Which means $p \nmid an$

According to theorem 2.1 on textbook

$\forall x, d \in \mathbb{Z}, \exists q, r \in \mathbb{Z}\ s.t.\ x = qd + r \wedge 0 \leq r < x$

We can conclude that $0 \leq r_p(an) < p$

Because $p \nmid an$

Then $0 < r_p(an) < p$

Which means $\{r_p(an) | n \in T\} \subseteq T$ ■

(b)

Proof: Let a, p $\in \mathbb{R}$ with p prime and gcd(a, p) = 1

Let T = {1, ..., p - 1}

Let n $\in$ T

Assume $n_1 \neq n_2$ and $n_1, n_2 \in T$

Use contradiction

Assume $r_p(an_1) = r_p(an_2)$

According to theorem 2.1 on textbook

$\forall x, d \in \mathbb{Z}, \exists q, r \in \mathbb{Z}\ s.t.\ x = qd + r \wedge 0 \leq r < x$

We know that $\exists q_1, r \in \mathbb{Z}\ s.t.\ an_1 = q_1 d + r$

$\exists q_2, r \in \mathbb{Z}\ s.t.\ an_2 = q_2 d + r$

WTS $\exists q_3 \in \mathbb{Z}\ s.t.\ an_1 - an_2 = q_3 d$

Take $q_3 = q_1 - q_2$

Then $q_3 d = q_1 d - q_2 d$

$= q_1 d + r - q_2 d + r$

$= an_1 - an_2$

Which means that $r_p(an_1 - an_2) = r_p(a(n_1 - n_2)) = 0$

Case1: If $n_1 - n_2 = 1$

Then $r_p(a) = 0$

Which means that p | a

Obviously it can't be true

Case2: If $n_1 - n_2 \in$ [2, p – 1]

According to the definition of Prime

We know that $p \nmid (n_1 - n_2)$

Which means gcd(p, $(n_1 - n_2)$) = 1

Then $\exists s_1, t_1 \in \mathbb{Z}\ s.t.\ s_1 p + t_1(n_1 - n_2) = 1$

Similarly $\exists s_2, t_2 \in \mathbb{Z}\ s.t.\ s_2 p + t_2 a = 1$

WTS $\exists s_3, t_3 \in \mathbb{Z}\ s.t.\ s_3 p + t_3 a(n_1 - n_2) = 1$

Let $s_3 = s_1 s_2 + t_1 s_2 p + t_2 s_1 a$

Let $t_3 = t_1 t_2$

Then $s_3 p + t_3 a(n_1 - n_2)$

$= (s_1s_2 + t_1s_2p + t_2s_1a)p + t_1t_2a(n_1 - n_2)$
$= (s_1p+t_1(n_1 - n_2)) + (s_2p+t_2a)$
$= 1$

Which means $p \nmid a(n_1 - n_2)$

And Then $r_p(an_1 - an_2) \neq 0$

Which isn't matches our consumption

As a result, our assumption $r_p(an_1) = r_p(an_2)$ must be wrong

And so, if $n_1 \neq n_2$ and $n_1, n_2 \in T$, then $r_p(an_1) \neq r_p(an_2)$ ■

(c)

Proof: Let a, p $\in \mathbb{R}$ with p prime and gcd(a, p) = 1

Let T = {1, …, p - 1}

Let n $\in$ T

From Claim b we know that if $n_1 \neq n_2$ and $n_1, n_2 \in T$, then $r_p(an_1) \neq r_p(an_2)$

Which means every different n $\in$ T matches one and only one $r_p(an) \in T$

So we can say the number of n is equal to the number of $r_p(an)$

Which means $\left|\left\{r_p(an) \middle| n \in T\right\}\right| = |T|$

(d)

Proof: Let a, p $\in \mathbb{R}$ with p prime and gcd(a, p) = 1

Let T = {1, …, p - 1}

Let n $\in$ T

We know that for finite sets A and B if A $\subseteq$ B then |B| = |B\A| - |A|

Which means that |T| = $|T \setminus \left\{r_p(an) \middle| n \in T\right\}|$ - $|\left\{r_p(an) \middle| n \in T\right\}|$

From Claim c we know that $\left|\left\{r_p(an) \middle| n \in T\right\}\right| = |T|$

Which means that $|T \setminus \left\{r_p(an) \middle| n \in T\right\}|$ = 0

So $\left\{r_p(an) \middle| n \in T\right\}$ = T ■

(e)

Proof: By Claim 3 we know that $\left|\left\{r_p(an) \middle| n \in T\right\}\right| = |T|$

By Claim 4 We know that $\left\{r_p(an) \middle| n \in T\right\}$ = T

All of these shows that each $r_p(an) \in T$ matches one and only one different $n \in T$, and there aren't any spare elements exists

Which means that $r_p(a)r_p(2a) \dots r_p(a(p-1)) = 1 \bullet 2 \bullet \dots \bullet (p-1)$

Hence $\prod_{i=1}^{i=p-1} r_p(an) = \prod_{i=1}^{i=p-1} i$ ■

(f)

Proof: Let a, p $\in \mathbb{R}$ with p prime and gcd(a, p) = 1

Let T = {1, …, p - 1}

From claim b we know that if $n_1 \neq n_2$ and $n_1, n_2 \in T$, then $r_p(an_1) \neq r_p(an_2)$

From Claim c we know that $\left|\left\{r_p(an) \middle| n \in T\right\}\right| = |T|$

From claim d we know that $\left\{r_p(an) \middle| n \in T\right\}$ = T

All of this shows that for $i, \in \{1,2,\dots,p-1\}$

$an_i \equiv n_i(\text{modp})$
By the consequence of 2.8 we know that
if for $i \in \{1,2,\ldots,k\}$ $a_i \equiv b_i(\text{modp})$, then $\prod_1^k a_i \equiv \prod_1^k b_i(\text{modp})$
We can conclude that $\prod_1^{p-1} an_i \equiv \prod_1^{p-1} n_i(\text{modp})$
Which means that $p|(an_i - n_i)$
Which equals to p|(a – 1)
By the consequence of 2.8 we know that
if for $i \in \{1,2,\ldots,k\}$ $a_i \equiv b_i(\text{modp})$, then $\prod_1^k a_i \equiv \prod_1^k b_i(\text{modp})$
So if $a \equiv 1(\text{modp})$, then $\prod_1^{p-1} a \equiv \prod_1^{p-1} 1(\text{modp})$
Then $p|(a^{p-1} - 1^{p-1})$
$p|(a^{p-1} - 1)$
Which means that $r_p(a^{p-1}) = 1$, as we need to prove ■

(g)
Proof: Let a, p $\in \mathbb{R}$ with p prime and gcd(a, p) = 1
Let T = {1, …, p - 1}
According to Claim f we know that $r_p(a^{p-1}) = 1$
Which means that $r_5(a^4) = 1$
By the consequence of 2.8 we know that
if for $i \in \{1,2,\ldots,k\}$ $a_i \equiv b_i(\text{modp})$, then $\prod_1^k a_i \equiv \prod_1^k b_i(\text{modp})$
By example 2.18 we know that
$\forall a,b,c,d,e \in \mathbb{Z}, a \equiv c(\text{mode}) \land b \equiv d(\text{mode}) \Longrightarrow ab \equiv cd(\text{mode})$
We can conclude
$\forall a,c,k \in \mathbb{Z}, a \equiv c \Longrightarrow a^k \equiv c^k(\text{mode})$
Then $5|((a^4)^{25} - (1^4)^{25})$
$5|(a^{100} - 1^{100})$
$5|(a^{100} - 1)$
Which means that $r_5(a^{100}) = 1$, as we need to prove ■

Q5
(a)
Translation: $\forall k \in \mathbb{N}, \exists n \in \mathbb{N}$ s.t. $\neg\text{Prime}(n) \land \neg\text{Prime}(n+1) \land \ldots \land \neg\text{Prime}(n+k)$
Proof: Let $k \in \mathbb{N}$
Let n = (k + 2)! + 2
Then:
2 | n = (k + 2)! + 2
3 | n + 1 = (k + 2)! + 3
4 | n + 2 = (k + 2)! + 4
5 | n + 3 = (k + 2)! + 5
6 | n + 4 = (k + 2)! + 6
…
k + 2 | n + k = (k + 2)! + k + 2
Which prove $\neg\text{Prime}(n+2) \land \ldots \land \neg\text{Prime}(n+k)$

So far we have proved that

$\forall k \in \mathbb{N}, \exists n \in \mathbb{N} \text{ s.t. } \neg\text{Prime}(n) \wedge \neg\text{Prime}(n+1) \wedge \ldots \wedge \neg\text{Prime}(n+k)$ ■

(b)

Proof: Let $n \in \mathbb{N}^+$

Case 1: If n! + 1 is a prime

Take p = n! + 1

Then n < p < n! + 2.

Case 2: If n! + 1 is not a prime

We know that $n \in \mathbb{N}^+$

If n = 1

Then n! + 1 = 2 is a prime, which is contradictory to the statement

So n > 1

Then n! + 1 > 2

Since the smallest prime is 2

We can conclude that there always exists a prime p which is less than n! + 1

If p < n

According to the theorem that every composite number can be divided by several primes

We know that p | n! + 1

Also p | n!

We can conclude that p | n! + 1 – n! = 1

This is impossible because no number can divide 1 except 1 itself

As a result our assumption $p \leq n$ is impossible

Which means that n < p < n! + 1

So far we have proved that

For any positive natural number n there exists a prime p with n < p < n! + 2 ■