1.

a)

p	q	r	$p \vee q$	$(p \vee q) \Rightarrow r$
T	T	T	T	T
T	T	F	T	F
T	F	T	T	T
T	F	F	T	F
F	T	F	T	F
F	T	T	T	T
F	F	T	F	T
F	F	F	F	T

b)

$$(p \vee q) \Rightarrow r$$
$$= \neg(p \vee q) \vee r$$
$$= (\neg p \wedge \neg q) \vee r$$

2.

a) my statement: $\forall\, m, n \in \mathbb{N}, [7|(m-5) \wedge 7|(n-2)] \Longrightarrow 7|(mn-3)$

I believe the statement:

Proof: Let m,n$\in \mathbb{N}$, assume 7|(m-5), that $\exists\, k_1 \in \mathbb{Z}, 7 \times k_1 = m-5.$ Let k_1 be such a value.

Also, assume 7|(n-2) that is $\exists\, k_2 \in \mathbb{Z}, 7 \times k_2 = n-2.$ Let k_2 be such a value.

Let k_3=7k_1k_2+2k_1+5k_2+1

Then 7k_3=49k_1k_2+14k_1+35k_2+7

=(7k_1+5)(7k_2+2)-3

=mn-3 ■

b)converse: $\forall\, m, n \in \mathbb{N}, 7|(mn-3) \Longrightarrow [7|(m-5) \wedge 7|(n-2)]$

I disbelieve the converse:

Proof: Take m=10,n=1, so $m, n \in \mathbb{N}$, and $7|(mn-3)$

But $7 \nmid 5$and $7 \nmid -1$ that is $7 \nmid (m-5)$ and $7 \nmid (n-2)$

Hence, the converse is false. ■

3.

a)proof:

Let $F = \{f | f: D \to R \wedge |D| > 0 \wedge |R| > 0\}$The pigeonhole principle says that:

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

This is equal to $\forall f \in F, |D| > |R| \Longrightarrow \exists x, y \in D, x \neq y \wedge f(x) = f(y)$

We can define the question as a function f:A→B , domain A is the set of people at the party, range B is the set of the number of people each person shook hands with.

Since when a people shook hand with |A|-1 people, there will be no people have not shake hand with anybody. Vice versa. Hence the range B may be 0~|A|-2 or 1~|A|-1, so |B|≤|A|-1, hence |B|<|A|.

With the pigeonhole principle above, we can prove that $\exists x, y \in D, x \neq y \wedge f(x) = f(y)$ that is there are at least 2 people who shake hands with the same number of other people. ■

4.

a)Proof:

From the couse note we have this statement : $\forall n \in \mathbb{N}, \mathrm{Prime}(n) \Longrightarrow (n > 1 \wedge (\forall a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \Rightarrow n \nmid ab))$ and the proof of this statement is:

Let n $\in \mathbb{N}$. Assume that n is prime. We need to prove that n > 1
and that Atomic(n) are true.

For the first part, the definition of prime tells us immediately that n > 1.

For the second part, we want to prove that $(\forall a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \Rightarrow n \nmid ab)$,Let $a, b \in \mathbb{N}$ and assume that n $\nmid$ a and n $\nmid$ b. We want to prove
that n $\nmid$ ab.

We'll first prove that there exist r_3, $s_3 \in \mathbb{Z}$, r_3n + $s_3$ab = 1. By Claim
1 and the assumption that n is prime, there exist r_1, s_1, r_2, s_2 $\in \mathbb{Z}$ such
that r_1n + s_1a = 1 and r_2n + s_2b = 1. Let r_3 =$r_1 r_2$n + $r_2 s_1$a + $r_1 s_2$b
and s_3 = $s_1 s_2$.

Then we can multiply the first two equations to obtain:

(r_1n + s_1a)(r_2n + s_2b) = 1

$r_1 r_2 n^2$ + $r_2 s_1$an + $r_1 s_2$bn + $s_1 s_2$ab = 1

($r_1 r_2$n + $r_2 s_1$a + $r_1 s_2$b)n + $s_1 s_2$ab = 1

r_3n + $s_3$ab = 1

So then there exist r_3, $s_3 \in \mathbb{Z}$, r_3n+$s_3$ab = 1. Then using Claim 2 (and
again the assumption that n is prime), we can conclude that n $\nmid$ ab.

And the claim1 : $\forall n, m \in \mathbb{N}, \mathrm{Prime}(n) \wedge n \nmid m \Rightarrow (\exists r, s \in \mathbb{Z}, rn + sm = 1)$ which can be proved by the claim3 and claim 6 in the Tutorial4 worksheet

Claim 2: $\forall n, m \in \mathbb{N}, \mathrm{Prime}(n) \wedge (\exists r, s \in \mathbb{Z}, rn + sm = 1) \Rightarrow n \nmid m$ which can be proved by the claim 6 in the Tutorial4 worsheet.

Gcd(a,p)=1 and Prime(p) means $p \nmid a$ (same as the claim2 above)

And we also know that $p \nmid n$ for n is belong to T (T={1,...,p-1})

With the statement$\forall n \in \mathbb{N}, \mathrm{Prime}(n) \Longrightarrow (n > 1 \wedge (\forall a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \Rightarrow n \nmid ab))$ **showned above we can find that** $p \nmid an$. Hence rp(an) must be one of 1,....,p-1

In all, $\{r_p(an) | n \in T\} \subseteq T$. ■

b)Proof:

reduction ad absurdum:

assume that there are two distinct numbers n_1 and n_2 in T, that $r_p(an_1) = r_p(an_2)$

we also know that p| $an_1 - r_p(an_1)$ and p| $an_2 - r_p(an_2)$

so we can get the statement that p| a(n_1- n_2)

since n_1,$n_2 \in T$ and they are distinct so |n_1- n_2|$\in T$ *that is* (n_1- n_2) cannot be divisible by p, With the statement$\forall n \in \mathbb{N}, \mathrm{Prime}(n) \Longrightarrow (n > 1 \wedge (\forall a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \Rightarrow n \nmid ab))$ **showned above we can find that** $p \nmid (n_1 - n_2)$. And this is contradict to the conclusion we assumed. So the statement we assumed is not true . And we can get the result that If n_1 and n_2 are distinct numbers in T, then $r_p(an_1) \neq r_p(an_2)$■

c)Proof:

Let $\mathrm{F} = \{f | f: D \to R \land |D| > 0 \land |R| > 0\}$The pigeonhole principle says that:

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

since if n_1 and n_2 are distinct numbers in T, then $r_p(an_1) \neq r_p(an_2)$ (claim b) that meet OneToOne(f)

So $|T| \leq |\{r_p(an) | n \in T\}|$

since $\{r_p(an) | n \in T\} \subseteq T$ (claim a) so$|\{r_p(an) | n \in T\}| \leq |T|$

so *we can say* $|\{r_p(an) | n \in T\}| = |T|$ ■

d)Proof:

since For finite sets A and B if A⊆ B then |B|=|B\A| + |A| , both $\{r_p(an) | n \in T\}$ and T are finite sets and $\{r_p(an) | n \in T\} \subseteq T$(claim1) so $|T|=|T \setminus \{r_p(an) | n \in T\}| + |\{r_p(an) | n \in T\}|$

since $|\{r_p(an) | n \in T\}| = |T|$ we can get that $|T \setminus \{r_p(an) | n \in T\}|=0$ that means $T \setminus \{r_p(an) | n \in T\}=\emptyset$ hence we can conclude that $\{r_p(an) | n \in T\}$=T ■

e)Proof:

Since i = 1~P-1 so i is all the element of T. So $\prod_{\mathrm{i}=1}^{\mathrm{i=p\text{-}1}} r_p(a\mathrm{i})$ is the product of all elements in $\{r_p(an) | n \in T\}$ and $\prod_{\mathrm{i}=1}^{\mathrm{i=p\text{-}1}} \mathrm{i}$ is the product of all elements in T.

We also know that $\{r_p(an) | n \in T\}$=T (claim d) , so the the product of all elements in $\{r_p(an) | n \in T\}$ is equal to the product of all elements in T.

Hence we can prove that $\prod_{\mathrm{i}=1}^{\mathrm{i=p\text{-}1}} r_p(a\mathrm{i}) = \prod_{\mathrm{i}=1}^{\mathrm{i=p\text{-}1}} \mathrm{i}$ ■

f)Proof:

As a consequence of Example 2.18, if for $\mathrm{i} \in \{1,2,\ldots,\mathrm{k}\}\ \mathrm{a_i} \equiv \mathrm{b_i} (\mathrm{mod\ p}), \mathrm{then} \prod_1^{\mathrm{k}} \mathrm{a_i} = \prod_1^{\mathrm{k}} \mathrm{b_i}$(mod p).

We can find that $\prod_{\mathrm{i}=1}^{\mathrm{i=p\text{-}1}} \mathrm{a_i} \equiv \prod_{\mathrm{i}=1}^{\mathrm{i=p\text{-}1}} r_p(\mathrm{a_i})\ (\mathrm{mod\ p})$ since $\mathrm{i} \in \{1,2,\ldots,\mathrm{p\text{-}1}\}\ r_p(\mathrm{a_i}) \equiv \mathrm{a_i}(\mathrm{mod\ p})$.

We also know that $\prod_{\mathrm{i}=1}^{\mathrm{i=p\text{-}1}} r_p(\mathrm{a_i}) = \prod_{\mathrm{i}=1}^{\mathrm{i=p\text{-}1}} \mathrm{i}\ \ (\mathrm{claim\ e})$

So $\prod_{\mathrm{i}=1}^{\mathrm{i=p\text{-}1}} \mathrm{a_i} \equiv \prod_{\mathrm{i}=1}^{\mathrm{i=p\text{-}1}} \mathrm{i}$ (mod p)

So $\mathrm{p} | (\prod_{\mathrm{i}=1}^{\mathrm{i=p\text{-}1}} \mathrm{a_i} - \prod_{\mathrm{i}=1}^{\mathrm{i=p\text{-}1}} \mathrm{i})$

That is p|[a^{p-1} ×1×2×3×.... ×(p-1)-1×2×3×... ×(p-1)]
That is p|[(a^{p-1}-1) × [1×2×3×.... ×(p-1)]]
Since none of {1,2,3...(p-1)} can be divisible by p, (a^{p-1}-1) must can be divisible by p.
As an extension of Example 2.14, that for any k>1, if prime p∤ b_1 ∧p∤ b_2...∧p∤ b_k, then p∤ $(b_1 \times b_2 \times \ldots \times b_k)$ so p∤ a^{p-1} since p∤ a
So (a^{p-1}-1) must can be divisible by p means 1≡ a^{p-1}(mod p)
Since 1 is the smallest integer grater than zero we can find that $r_p(a^{p-1}) = 1$■

g)Proof:
Since a is an arbitrary natural number that is not divisible by 5 that means gcd(a,5)=1
And we all know that 5 is a prime number since it can only be divisible by 1 or 5.
So we can get the conclusion that $r_5(a^4) = 1$ (claim f) that is 1≡ a^4(mod 5)
As a consequence of Example 2.18, if for $i \in \{1,2,\ldots,k\}$ $a_i \equiv b_i(\text{mod p})$, then $\prod_1^k a_i = \prod_1^k b_i$(mod p). so $1^{25} \equiv {a^4}^{25}$(mod 5) that is $1 \equiv a^{100}$(mod 5)
Since 1 is the smallest integer grater than zero we can find that $r_5(a^{100}) = 1$■

5.
a)Proof:
Let k∈ ℕ, take n=2+(k+2)!
We can write n,n+1,...,n+k as n+a(a∈ $[0,k]$ and $a \in \mathbb{Z}$)
So n+a $= 2 + (k+2)! + a = (2+a) + (k+2)!$
Since a∈ $[0,k]$,so (2+a) ∈ $[2, k+2]$
So we can write n+a=(2+a)[1×2×3×(1+a) ×(3+a) ×(4+a) ×... ×(k+2)+1]
So n+a can be divisible by (2+a) which does not equal to 1 or n+a for (2+a)>1 since a∈ $[0,k]$ and n>2 since n=2+(k+2)! and (k+2)!>1 for k∈ ℕ
So we can say n+a is composite.
Hence for any k∈ ℕ there is some n∈ ℕ such that n,n1, ...n+k are composite. ■

b)Proof:
Let n>0 and n∈ ℕ
Take a look at n!+1 ,
If n!+1 is a prime number then p=n!+1 since n<n!+1<n!+2 (n>0) the statement is proved.
If n!+1 is not a prime number then n!+1 must can be writed as a$\times b \times c \ldots$.(a,b,c...is prime number) and a,b,c,...>n for the reason below:
We assume that there exist a number p∈{a,b,c...} and p$\leq$ n then p|n! and p|n!+1
So p|n!+1-n! that is p|1 and this is impossible for p is a prime so p>1. So what we assumed is false that is $\forall p \in \{a, b, c \ldots\}, p > n$
Since n!+2>n!+1= a$\times b \times c \ldots$.(a,b,c...is prime number) so $\forall p \in \{a, b, c \ldots\}, p <$ n! +

2 and p is a prime.
In all $\forall p \in \{a, b, c \ldots\}, n < p < n! + 2$ and p is a prime and this meet the statement.

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