Mock exam

Q1

a) For integers a, b, we say "a divides b" if there exists $c \in \mathbb{Z}$ such that

$$b = c\,a$$

This is written as $a \mid b$, or $a \nmid b$ when this is not true.

Let $a, b, c \in \mathbb{Z}$ and assume that $a \mid b$ and $a \mid c$.

From the definition above this means there exists $\beta, \gamma \in \mathbb{Z}$ that satisfy.

$$b = a\beta \quad \text{and} \quad c = a\gamma.$$

Let $m, n \in \mathbb{Z}$.

$$mb + nc = m a\beta + n a\gamma, \quad \text{replacing } b, c \text{ with the above}$$

$$= a(m\beta + n\gamma).$$

Clearly $m\beta + n\gamma \in \mathbb{Z}$ since all four m, β, n, γ are integers and so $a \mid (mb+nc)$ by the def. of divisibility. $\blacksquare$

b) First let $n=1$, then

$$2^{3n} - 1 = 2^3 - 1 = 7.$$

and clearly $7 \mid 7$. So the base case of the induction is true.

Now assume $\boxed{7 \mid \boxed{2^{3k} - 1}}$ for some $k \geq 1$ and consider

$$2^{3(k+1)} - 1 = 2^{3k+3} - 1$$

$$= 2^3 \cdot 2^{3k} - 1$$

$$= 2^3 \left(2^{3k} - 1\right) + 7.$$

Now notice that this last expression is a linear combination of $2^{3k}-1$ and 7, both of which are divisible by 7.

Therefore, by result from part (a),

$$7 \mid 2^{3(k+1)}-1.$$

So we have shown that

$$7 \mid 2^{3k}-1 \implies 7 \mid 2^{3(k+1)}-1,$$

and by induction, this proves that

$$\forall n \geq 1 \quad 7 \mid 2^{3n}-1.$$

c) gcd(a,b) ~~is~~ is the greatest common divisor of a and b, i.e. the greatest integer d such that

$d \mid a$ and $d \mid b$.

Consider the set L, defined by

$$L = \{ ma + nb : m, n \in \mathbb{Z} \}$$

then $\gcd(a,b)$ is the smallest positive element of L.

d). Let $a, b, c \in \mathbb{Z}$.

Assume $\boxed{\gcd(a,b) = 1}$ and $a \mid c$ and $b \mid c$.

This means there exist $\alpha, \beta \in \mathbb{Z}$. such that $c = \alpha a$, $c = \beta b$.

There exists $x, y \in \mathbb{Z}$ such that $1 = xa + yb$

$$\Rightarrow \quad c = xac + ybc$$

$$= xa\beta b + yb\alpha a$$

$$= ab(x\beta + y\alpha)$$

$$\Rightarrow \quad c = \underset{\sim}{ab}\underbrace{(\quad\checkmark\quad)}_{\in \mathbb{Z}}.$$

$$\Rightarrow \quad ab \mid c.$$

Note the term in the bracket, $x\beta + y\alpha$ is clearly an integer. $x, \beta, y, \alpha \in \mathbb{Z}$.

Therefore $ab \mid c$ as required

$\blacksquare$

Q2

(a). Euclid's proof of infinitely many primes.

<u>Proof</u> (Proof by contradiction).

First assume there are only a finite number of primes and that they are all listed as.

$p_1, \ldots, p_r$

Then consider the integer M defined as

$$M = (p_1 p_2 p_3 \ldots p_r) + 1$$

$$= 1 + \prod_{j=1}^{r} p_j$$

By a result from the unit M factorises ~~~~ into primes. So let q be a prime factor of M.

i.e. $q \mid M$.

But by assumption $q = p_i$, for some $i = 1, \ldots, r$. This means.

$$q \mid p_1 p_2 \ldots p_r$$

So by the divisibility of linear combinations. $q \mid 1$, since.

$$1 = M - (p_1 p_2 \ldots p_r)$$

But this is a contradiction since $q > 1$ so cannot divide 1.

So our initial assumption itself must be false, so therefore there are an infinite number of primes. ∎

(b) Euclid's lemma was crucial for Fundamental theorem of Arithmetic.

<u>Proof of Euclid's lemma</u>

Let $a, b \in \mathbb{Z}$. Let p be a prime number, satisfying $p \mid ab$.

From logic.

$$(A \text{ OR } B) \equiv \neg A \Rightarrow B$$

If $p \mid a$ we are done.

otherwise we can assume

$p \nmid a$, ie. $\gcd(p,a) = 1$,

since p is a prime and only has the factors 1 and p.

This means there exist $x, y \in \mathbb{Z}$. such that.

$$1 = xp + ya.$$

$$\Rightarrow \quad b = xpb + yab.$$

$\Rightarrow$ $p \mid b$, since we have b as a linear combination of p and ab both of which are divisible by p.

This has shown.

$$p \nmid a \Rightarrow p \mid b.$$

which is equivalent to.

$$p \mid a \text{ or } p \mid b. \quad \blacksquare$$

(c)

Claim: 2^m+1 is prime $\Rightarrow m=2^n$ for some $n\in\mathbb{Z}$.

Proof: We will the contrapositive instead.

$$(A\Rightarrow B) \equiv ((\neg B)\Rightarrow(\neg A))$$

contrapositive of $A\Rightarrow B$

which is the statement.

If $m\neq 2^n$ for some $n\in\mathbb{Z}$

then 2^m+1 is

composite.

We assume that m can be expressed as

$m = \underbrace{2^n \cdot s}$, for some odd $s > 1$

$$2^m + 1 = 2^{2^n \cdot s} + 1$$

$$= \left(2^{2^n}\right)^s - (-1)^s$$

$$= \underbrace{\left(2^{2^n} + 1\right)}_{m} \underbrace{\left(\sum_{j=0}^{s-1} \left(2^{2^n}\right)^{s-1-j} (-1)^j\right)}$$

$$\Rightarrow 2^m + 1 = \underset{\in \mathbb{Z}}{\underline{\qquad}} \times \underset{\in \mathbb{Z}}{\underline{\qquad}}$$

$\Rightarrow 2^m + 1$ is composite.

since we've produced a non-trivial integer factorisation of 2^m+1.

since $2^{2^n}+1 > 1$

and $2^{2^n}+1 < 2^m+1$.

This proves the contrapositive and hence the original result.

Q3(a).

For a natural number $n > 0$ and integers a, b we say "a is congruent to b modulo n" written as $a \equiv b \pmod{n}$ iff.

$$n \mid a - b.$$

And further, $a \equiv b \pmod{n}$ iff a, b. leave the <u>same</u> smallest positive remainder after division by n.

i.e. If $a = q_1 n + r_1$ $\quad 0 \leq r_1, r_2 < n$

$$b = q_2 n + r_2$$

then

$$a \equiv b \pmod{n} \iff r_1 = r_2.$$

b) Results show $+$ and $\cdot$ fit well with congruence modulo n.

Assume $a \equiv a'$, $b \equiv b' \pmod{n}$.

Claim 1. $a+b \equiv a'+b' \pmod n$.

2. $ab \equiv a'b' \pmod n$.

Proofs We have to show.

$$n \mid (a+b)-(a'+b').$$

and $n \mid ab - a'b'$

We can assume $n \mid a-a'$ and $n \mid b-b'$

$$(a+b)-(a'+b') = \boxed{(a-a')+(b-b')}$$

Secondly.

$$ab - a'b' = (a-a')(b-b') - 2a'b' + ab' + a'b.$$

$$= \boxed{(a-a')(b-b') + b'(a-a') + a'(b-b')}$$

Notice that both final RHS are lin. combs. of $a-a'$ and $b-b'$ and so are divisible by n, by the divisibility of linear combinations result.

Therefore $n \mid (a+b)-(a'+b')$ and $n \mid ab - a'b'$ as required. $\blacksquare$

(c). For a positive integer $n \geq 1$ $\phi(n)$ is defined as.

$\phi(n) =$ number of j such that $1 \leq j \leq n$ and $\gcd(j,n) = 1$.

moreover

$$\phi(n) = |U(n)| = |\mathbb{Z}_n^{\times}|.$$

Claim. For a prime p.

$$\phi(p^n) = p^{n-1}(p-1).$$

<u>Proof:</u>

Consider $1, 2, 3, \dots, p^n$

We will count the integers here that are not coprime to p^n and so indirectly counting the ones that are.

Notice that since p is prime.

$$\gcd(m, p^n) \neq 1 \iff p \mid m$$

The multiples of p in the top list are

$$p, 2p, 3p, \dots, p^{n-1} \cdot p$$

Clearly there are p^{n-1} numbers in this list.

So the number of integers in the top list that are coprime to p is therefore

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

want $a^{-1} \pmod{n}$

a^{-1} exists iff $\gcd(a,n)=1$.

find Bezout's identity

$$xa + yn = 1$$

$$\Longleftrightarrow \quad xa = -yn + 1 \equiv 1 \pmod{n}$$

$$x \equiv a^{-1} \pmod{n}$$

$$a^s - b^s$$

$$= (a-b) \sum_{j=0}^{s-1} a^{s-1-j} b^j$$

$$= (a-b)\left(a^{s-1} + a^{s-2} b + a^{s-3} b^2 + \dots + a b^{s-2} + b^{s-1}\right)$$