Coursework 1

15 October 2019 11:17

1a) Prove that if the square of integer z is divisible by 17, then z is divisible by 17.

Solution:

For: $z^2 = 17a$

$z = \sqrt{17 \cdot a}$

$z = \sqrt{17}\sqrt{a}$ as 17 is a prime number, $\sqrt{17}$ is irrational.

as $\sqrt{17}$ is irrational, for z to be an integer, $\sqrt{a}$ can be rewritten as; $a = \sqrt{17}\,b$,

Giving; $z = \sqrt{17}\sqrt{17}\,b$

$z = 17b$ hence, z is divisible by 17

1b) Prove that $\sqrt{17}$ is irrational;

Solution

Assume $\sqrt{17}$ is rational;

$\sqrt{17} = \frac{a}{b}$ where $b \neq 0$; $a, b \in \mathbb{Z}$; a, b have no common factors

$17 = \frac{a^2}{b^2}$

$a^2 = 17b^2$ 17 is prime, $\therefore 17 \mid a^2$, $\therefore$ by (1a): $17 \mid a \rightarrow a = 17k$

Subbing in; $17 = \frac{(17k)^2}{b^2} = \frac{17^2k^2}{b^2}$

$b^2 = 17k^2$ b is also divisible by 17

But a and b cannot both have a common factor of 17 if rational.

This is a contradiction hence $\sqrt{17}$ is irrational

2a) Give an example of a function $g: \mathbb{C} \rightarrow \mathbb{C}$ that is injective but not surjective.

Solution: $g(x) = 2x$

2b) Prove that $|Z| = |E|$ by defining an explicit bijection.

Solution:

Inverse of $g(x) = 2x$ exists: $g^{-1}(x) = \frac{1}{2}x$. hence $g(x)$ is a bijection.

The domain of $g(x)$ can be defined across the integers Z.

For any x a unique $g(x)$ exists. $\rightarrow$ $|Z| \leq |E|$

3a) Prove R is reflexive:

Solution: R is reflexive if $((a,b),(a,b)) \in R \quad \forall (a,b) \in A$

for $(a,b)R(c,d)$ where $ad = bc$ in the case $((a,b)(a,b))$

$ab = ab$ which is a tautology, hence R is reflexive

3b) Prove R is symetric

Solution: R is symetric iff $((a,b),(c,d)) \in R \rightarrow ((c,d),(a,b)) \in R \quad \forall a,b,c,d$

$ad = bc \rightarrow cb = ad$ as multiplication is commutative, R is symetric

3c) Prove R is transitive

Solution: R is transitive iff $((a,b),(c,d)) \in R \wedge ((c,d),(e,f)) \in R \rightarrow ((a,b),(e,f)) \in R \quad \forall a,b,c,d,e,f \in A$.

From $ad = bc \wedge cf = de$;

$a = \frac{bc}{d}, b = \frac{ad}{c}$

$c = \frac{ad}{b} = \frac{de}{f}$,

$d = \frac{cf}{e} = \frac{bc}{a}$,

$e = \frac{cf}{d}, f = \frac{de}{c}$

$\rightarrow$

$ad = bc$ try to replace d or c in terms of a,b,e,f

$a\frac{cf}{e} = bc$ Substituting d

$af = be$ Canceling out

, hence R is transitive

4a) Prove by induction that for every positive integer n; $\sum_{j=1}^{n} j2^j = (n-1)2^{n+1} + 2$

Solution

case of $n = 1$;

$RHS = \sum_{j=1}^{(1)} j2^j = 2$

$$RHS = \sum_{j=1}^{1} j2^j = \underline{2}$$

$$LHS = (1-1)2^{(1)+1} + 2 = \underline{2}$$

RHS = LHS ∴ holds for $n=1$

Assume for $n=k$ in the case of $n=k+1$;

$$RHS = \sum_{j=1}^{k+1} j2^j$$

$$= \sum_{j=1}^{k} j2^j + (k+1)2^{(k+1)}$$

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

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

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

$$= 2^{(k+2)}k + 2$$

$$= 2^{[(k+1)+1]}((k+1)-1) + 2 = LHS$$

b) Using fermats little theorem compute $11^{14} \bmod 7$

Solution:

FLT gives; $11^6 = 1 \pmod 7$

$$\rightarrow 11^{14} = 11^{6\cdot 2+2} = (11^6)^2 \cdot 11^2$$

$$\equiv (1)^2 \cdot 121$$

$$\equiv \underline{2 \pmod 7}$$

5) Assume a, b, m are positive integers and $d = \gcd(a, m)$. Prove the congruence $ax \equiv b \pmod m$ has integer solution x if $d \mid b$.

Solution:

$$ax = b \pmod m$$

iff $ax - b \mid m$

hence $ax - b = my$

rearranging; $ax - my = b$

as $d = \gcd(a,m)$, $d \mid a$ and $d \mid m$, meaning the equation can be

rearranging; $ax - my = b$

as $d = gcd(a, m)$, $d \mid a$ and $d \mid m$, meaning the equation can be rewritten as; $dsx - dty = b$

$d(sx - ty) = b$

$sx - ty = b/d$ b/d must be an integer, hence solutions exist iff b/d.

(I think) we have proved the stronger case that $ax \equiv b \pmod m$ if and only if $d \mid b$. Hence if $d \mid b$ then integer solution exists