

1. Setting  $k = 1$ , we get  $1 = \frac{1-(1+1)q+(1)q^2}{(1-q)^2}$

Which we see is true as  $(1 - q)^2 = 1 - 2q + q^2$  and  $q \neq 1$

Assume the statement is true for  $k = n$

i.e.  $1 + 2q + 3q^2 + \dots + nq^{n-1} = \frac{1-(n+1)q^n+nq^{n+1}}{(1-q)^2}$

Then we have,

$$\begin{aligned} 1 + 2q + 3q^2 + \dots + nq^{n-1} + (n+1)q^n &= \frac{1-(n+1)q^n+nq^{n+1}}{(1-q)^2} + (n+1)q^n \\ &= \frac{1 - (n+1)q^n + nq^{n+1} + (1 - 2q + q^2)(n+1)q^n}{(1-q)^2} = \frac{1 - (n+2)q^{n+1} + (n+1)q^{n+2}}{(1-q)^2} \end{aligned}$$

QED

2.a.  $45 = 9 * 5$ . Since 9 and 5 are both less than 43, both occur as separate factors in  $43!$ , or  $43! = 43 * 42 * 41 * \dots * 9 * \dots * 5 * \dots * 1$

Therefore  $43! \equiv 0 \pmod{45}$

2.b.  $3^2 \equiv 9 \equiv -1 \pmod{10}$ .

Thus,  $3^{2014} \equiv (-1)^{1007} \equiv -1 \equiv 9 \pmod{10}$

i.e. 9 is the last digit of the number

3. Instead of  $p_1^{k_1} p_2^{k_2}$  we shall refer it to as  $n = p^a q^b$ . Now any divisor of  $n$  will look like  $p^r q^s$  where  $r \leq a, s \leq b$ . Thus, if any number had gcd not 1 with  $n$ , then the gcd which is a divisor of  $n$ , should divide the chosen number. That is  $p^r q^s$  divides the number where not both  $r$  and  $s$  are 0. i.e either  $p$  divides the number or  $q$  divides the number, (or both in which case it is divisible by  $pq$  as they are coprime).

The number of multiples of  $p$  less than or equal to  $n$  is  $\frac{n}{p} = p^{a-1} q^b$ , given by  $\{p*1, p*2, \dots, p*\frac{n}{p}\}$

Similarly. The number of multiples of  $q$  less than or equal to  $n$  is  $\frac{n}{q} = p^a q^{b-1}$ , given by  $\{q*1, q*2, \dots, q*\frac{n}{q}\}$

Similarly. The number of multiples of  $pq$  less than or equal to  $n$  is  $\frac{n}{pq} = p^{a-1} q^{b-1}$ , given by  $\{pq*1, pq*2, \dots, pq*\frac{n}{qp}\}$

So the number of numbers which are divisible by  $p$  or  $q$  will be  $p^{a-1} q^b + p^a q^{b-1}$ , but we have counted the multiples of  $pq$  twice, so we subtract them once. i.e.  $p^{a-1} q^b + p^a q^{b-1} - p^{a-1} q^{b-1}$

So,  $\phi(n) = n - (p^{a-1} q^b + p^a q^{b-1} - p^{a-1} q^{b-1})$

$= p^a q^b - p^{a-1} q^b - p^a q^{b-1} + p^{a-1} q^{b-1}$

$= (p^a - p^{a-1})(q^b - q^{b-1})$

4. Let  $z_1 = a + ib$  and  $z_2 = c + id$ , where  $a, b, c, d$  are reals. Then,

a.  $(a - ib)(c - id) = (ac - bd) - i(ad + bc) = ac - bd + i(ab + bc) = \overline{(a + ib)(c + id)}$

b.  $|z_1 z_2|^2 = (z_1 z_2) \overline{z_1 z_2} = z_1 z_2 \bar{z}_1 \bar{z}_2 = (z_1 \bar{z}_1)(z_2 \bar{z}_2) = |z_1|^2 |z_2|^2$ .  
 Since  $|z|$  is always a positive real, this implies  $|z_1 z_2| = |z_1| |z_2|$

5. Let  $z^3 = t$ , then the equation turns to  $0 = t^2 + 7t - 8 = (t - 1)(t + 8)$ .

**Case 1**  $t - 1 = 0$ , then  $z^3 = t = 1$ . Obviously we see that  $z = 1$  is a solution.

Thus 1 is a root of  $z^3 - 1$ , thus,  $z^3 - 1 = (z - 1)(z^2 + z + 1)$ .

Solving the quadratic we get that  $z = \frac{-1 \pm i\sqrt{3}}{2}$  are also roots.

**Case 2**  $t + 8 = 0$ , setting  $-2s = z$ , equation becomes  $-8s^3 + 8 = 0$  or  $s^3 - 1 = 0$

This from case one we know implies  $\frac{z}{-2} = s = 1, \frac{-1 \pm i\sqrt{3}}{2}$

Thus all complex values for  $z$  are  $1, \frac{-1 \pm i\sqrt{3}}{2}, -2, 1 \pm i\sqrt{3}$

6. We can give a bijection from the power set of  $Z$  to the set of functions  $\{g : \mathbb{Z} \rightarrow \{1, 2\}\}$  as follows. For any  $S \subset Z$  We define  $f_S(t) = 1$  if  $t \in S$  and  $f_S(t) = 2$  otherwise.

To see that this is a bijection, we define another function that takes functions to subsets of  $Z$ , given by taking a function  $f$  to the set  $f^{-1}(1) = \{t \in Z | f(t) = 1\}$ .

It is easy to see that these processes are inverses of each other, proving a bijection.

7.  $f : S \rightarrow T$ , we define by

$$f(x) = \frac{x}{x-1} \text{ if } nx = 1 \text{ for some } n \in N,$$

$$f\left(\frac{2}{3}\right) = 0$$

$$f(x) = \frac{x}{2-2x} \text{ if } (2n+1)x = 2 \text{ for some } n \in N \text{ and } n \neq 1$$

$$f(x) = x, \text{ otherwise}$$

What we did was shifted the sequence  $\frac{1}{n}$  from  $n = 2$  onward to right by 1, and added one at the start

shifted the sequence  $\frac{2}{2n+1}$  to the right and fit 0 as the first term.

8. a True (constructible numbers form a field)

b False ( $2^{\frac{1}{3}}$  is not constructible)

c. False (it contains transcendental numbers)

d True (all rationals are constructible)

e. False ( $2^{\frac{1}{3}}$  is not constructible)

9.a  $\tan(\pi/30)$  is constructible if the angle  $\pi/30 = 6^\circ$  is constructible. Since  $3^\circ$  is constructible (Textbook theorem),  $6^\circ = 2 * 3^\circ$  is constructible.

9.b  $\sqrt[6]{8} = \sqrt{2}$ , therefore is constructible.  $\sqrt{1.3}$  is constructible (1.3 is constructible). And  $\sqrt[4]{3/5}$  is constructible, which implies, its square root  $\sqrt[4]{3/5}$  is constructible. Thus,  $\sqrt[4]{3/5} +$

$\sqrt{1.3}$  is constructible. And thus its inverse is constructible and thus  $\sqrt{2} \frac{1}{\sqrt[4]{3/5 + \sqrt{1.3}}}$  is constructible.

10.  $N = 21 = 3 * 7$ ,  $\phi(N) = (3 - 1)(7 - 1) = 12$   
 $ED \equiv 1 \pmod{\phi(N)}$   
 $5D \equiv 1 \pmod{12}$ ,  $5D \equiv 25 \pmod{12}$ .  
i.e.  $D \equiv 5 \pmod{12}$  or  $D = 5$   
 $R^D \equiv M \pmod{N}$   
As  $19 \equiv -2 \pmod{21}$ ,  
 $19^5 \equiv (-2)^5 \equiv -32 \equiv 10 \pmod{21}$   
Thus,  $M = 10$