

$$\tau(n) = \# \text{divisors of } n$$

a) show  $\tau(mn) = \tau(m)\tau(n)$  for  $(m, n) = 1$

Pf: look at prime factorization.

$$m = p_1^{e_1} \cdots p_k^{e_k}$$

$$\Rightarrow \tau(m) = (e_1 + 1) \cdots (e_k + 1)$$

b) show  $\sum_{d|n} \tau^3(d) = \left( \sum_{d|n} \tau(d) \right)^2$

$\underbrace{\hspace{10em}}_{f(n)} \qquad \underbrace{\hspace{10em}}_{g(n)}$

Pf: if  $f$  is multiplicative, then  
so is

$$g(n) = \sum_{d|n} f(d)$$

• so is  $f^2, f^3, \text{ etc.}$

by these facts,

$$\sum_{d|n} \tau^3(d) \leq \left( \sum_{d|n} \tau(d) \right)^2 \text{ are}$$

multiplicative.

It suffices to show that



$$f(p^k) = g(p^k) \quad \forall \text{ primes } p, \\ k \geq 0.$$

$$f(p^k) = \sum_{d|p^k} \tau^3(d)$$

$$= \sum_{j=0}^k \tau^3(p^j)$$

$$= \sum_{j=0}^k (j+1)^3$$

$$g(p^k) = \left( \sum_{d|p^k} \tau(d) \right)^2 = \left( \sum_{j=0}^k (j+1) \right)^2$$

remains to show that

$$\sum_{j=1}^{k+1} j^3 = \left( \sum_{j=1}^{k+1} j \right)^2 \quad \text{induction}$$

Prove that  $\sum_{k=1}^n k = \frac{n(n+1)}{2}$

~~PF: let  $P(n)$  be " $\sum_{k=1}^n k = \frac{n(n+1)}{2}$ "~~

~~therefore  $P(n+1)$  !!~~

~~"let the pigeons be, ...~~

~~let the pigeonholes be, ...~~

② Show that  $g \in \mathbb{Z}/_{257}\mathbb{Z} \sim 0$  is  
 a primitive root if and only if  
 $g^{128} \equiv -1 \pmod{257}$ .  $\mathbb{Z}/_p\mathbb{Z}^*$

note: 257 is prime!

$$p-1 = 256 = 2^8$$

$g$  is a p.r. iff  $\text{ord}(g) = p-1$   
 $= 256 = 2^8$

$$\text{ord}(g) \mid p-1 = 2^8 \Rightarrow \text{ord}(g) = 2^k$$

$g \neq 0$ .

for some  $k$ .

$$(g^{128})^2 = g^{256} = g^{p-1} \stackrel{\text{FLT}}{=} 1$$

$$\Rightarrow g^{128} = \pm 1 \pmod{p} \quad \left( \begin{array}{l} x^2 = 1 \text{ has} \\ \text{sols } \pm 1 \end{array} \right)$$

if  $g^{128} = 1$ , then  $\text{ord}(g) < 256$

$\Rightarrow g$  not p.r.

conversely, if  $g$  is not a p.r.

$$\Rightarrow \text{ord}(g) = 2^k, \quad k < 8$$

$$g^{128} = g^{2^7} = g^{2^k \cdot \overbrace{2^{7-k}}^{> 0}} = (g^{2^k})^{2^{7-k}} = 1^{2^{7-k}} = 1$$



(4) Show that for any  $k \geq 2$  the number  $\sum_{n=1}^{\infty} \frac{1}{k^{n!}}$  is transcendental.

Pf: See lecture notes (10? 11?)

$$\sum_{n=1}^{\infty} \frac{1}{10^{n!}} \text{ transcendental.}$$

$$\text{Idea: } x = \sum_{n=1}^{\infty} \frac{1}{k^{n!}}$$

$$\text{let } r_N = \sum_{n=1}^N 1/k^{n!} = \frac{a_N}{k^{N!}}$$

$$0 < \alpha - r_N = \sum_{n=N+1}^{\infty} 1/k^{n!} < 2/k^{(N+1)!}$$

thm

$$\frac{1}{k^{(N+1)!}} + \sum_{n=N+2}^{\infty} 1/k^{n!}$$

look at  
base  $k$ ?

$$\left( \frac{1}{k^{(N+2)!}} + \frac{1}{k^{(N+3)!}} + \dots \right)$$

$$= \frac{1}{k^{(N+2)!}} \left( 1 + \frac{1}{k^{(N+3)}} + \frac{1}{k^{(N+4)(N+3)}} \right)$$

$\leq$  geometric

$$\leq 2$$

QED

$$\text{Let } \underline{b_N} = K^{N!}$$

$$0 < \alpha - \frac{a_N}{K^{N!}} < \frac{2}{K^{(N+1)!}}$$

$$0 < \underline{\alpha - \frac{a_N}{b_N}} < \frac{2}{b_N^{N+1}} = \frac{2}{b_N} \cdot \frac{1}{b_N^N} \\ < \underline{1/b_N^N}$$

if  $\alpha$  were algebraic degree  $D$ ,  
this would have only finitely many  
solutions for  $N \geq D$

but we showed it has solutions  $\forall N$

③ Let  $(x_k, y_k)$  be the  $k$ -th solution to Pell's equation  $x^2 - Dy^2 = 1$

Show that the limit  $\lim_{k \rightarrow \infty} \frac{x_{k+1}}{x_k}$  exists.

Let  $(x_1, y_1)$  be the fundamental soln.

then

$$x_k + y_k \sqrt{D} = (x_1 + y_1 \sqrt{D})^k$$

$$\begin{aligned} \Rightarrow \underline{x_{k+1}} + y_{k+1} \sqrt{D} &= (x_k + y_k \sqrt{D})(x_1 + y_1 \sqrt{D}) \\ &= \underline{(x_1 x_k + y_1 y_k D)} \\ &\quad + (y_1 x_k + x_1 y_k) \sqrt{D} \end{aligned}$$

$$\frac{x_{k+1}}{x_k} = x_1 + y_1 D \frac{y_k}{x_k} \rightarrow x_1 + y_1 \sqrt{D}$$

$$x_k^2 - y_k^2 D = 1$$

$$\begin{aligned} \Rightarrow \left( \frac{x_k}{y_k} \right)^2 - D &= \frac{1}{y_k^2} \\ \Rightarrow \frac{x_k}{y_k} &\rightarrow \sqrt{D} \end{aligned} \quad \left. \begin{array}{l} \text{as } k \rightarrow \infty, \\ y_k \rightarrow \infty \end{array} \right\}$$