

18.781

10 Mar 2003

Exam Problem 4:  $p \geq 2$  primeNumerator of  $1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} = v$  is divisible by  $p$ .•  $\sum_{i=1}^{p-1} \frac{1}{i}$  is enough to show  $p \mid (p-1)! v$ •  $\sum_{i=1}^{p-1} \frac{(p-1)!}{i}$  Point:  $\left\{ \frac{(p-1)!}{i} \right\}_{i=1}^{p-1} \cup \{0\}$  is complete residue system.• congruence class of  $\frac{(p-1)!}{i}$  is unique class of #'s  $x$  s.t.  
 $x \cdot i \equiv -1 \pmod{p}$ .•  $\sum_{i \in S} r_i \equiv 1 + 2 + \dots + p-1 \pmod{p} = \frac{p(p-1)}{2}$  and  $\frac{(p-1)!}{2}$  is an integer since  $p$  an odd prime.Solving  $f(x) \equiv 0 \pmod{m}$ 

$$m = \prod p^{\alpha}$$

Look at  $f(x) \equiv 0 \pmod{p^{\alpha}}$ Prime power moduli:Thm (Hensel's Lemma) $f(x)$  polynomial with integer coeff, and say  $f(a) \equiv 0 \pmod{p^j}$  for some  $a \in \mathbb{Z}$ . If  $f'(a) \not\equiv 0 \pmod{p}$ , then  $\exists a_2$  with  $a_2 \equiv a \pmod{p^j}$  s.t.  
 $f(a_2) \equiv 0 \pmod{p^{j+1}}$ Lemma  $f(x)$  as above,  $k, a \in \mathbb{Z}$ . Then  $f^{(k)}(a)/k!$  is an integer.PF: It is enough to consider  $f(x) = cx^k$ 

$$f^{(k)}(a) = \underbrace{c \cdot (k-1) \cdot \dots \cdot (k-k+1)}_{k \text{ consecutive integers, so divisible by } k!} a^{k-k}$$

 $k$  consecutive integers, so divisible by  $k!$ Proof of Thm:  $a_2 = a + p^j$  for some  $t \in \mathbb{Z}$ 

$$f(a + p^j) = f(a) + t p^j f'(a) + \dots + t^2 p^{2j} \frac{f''(a)}{2!} + \dots + t^n p^{nj} \frac{f^{(n)}(a)}{n!}$$

Since for  $n \geq 2$ ,  $\frac{f^{(n)}(a)}{n!} p^{nj}$  is an integer divisible by  $p$ , we have

$$f(a + p^j) \equiv f(a) + t p^j f'(a) \pmod{p^{j+1}}$$

Want  $t p^j f'(a) \equiv -f(a) \pmod{p^{j+1}}$ .  $f(a) = p^j D$ , since  $f(a) \equiv 0 \pmod{p^j}$ .It is enough to solve  $t f'(a) \equiv -D \pmod{p}$ 

$$\text{i.e. } p \mid t f'(a) + D \Rightarrow p^{j+1} \mid p^j (t f'(a) + D).$$

Since  $f'(a) \not\equiv 0 \pmod{p}$  means  $f'(a)$  prime to  $p$ ,  $\exists y$  s.t.

$$y f'(a) \equiv 1 \pmod{p}.$$

Take  $t = -Dy$ .

$$\text{Take } a_2 = a + (-Dy) p^j.$$

Remark: If we have  $f(a) \equiv 0 \pmod{p}$  and  $f'(a) \not\equiv 0 \pmod{p}$ , then wecan solve  $f(x) \equiv 0 \pmod{p^j}$  for all  $j$ , since above  $f(a) \not\equiv 0 \pmod{p} \Rightarrow f'(a_2) \not\equiv 0 \pmod{p}$ .

Ex: Solve  $x^3 + x + 57 \equiv 0 \pmod{5^3}$ .

$$\text{mod } 5: x^3 + x + 2 \equiv 0 \pmod{5}$$

$$\text{Let } a_1 = -1.$$

$$\text{mod } 5^2: x^3 + x + 7 \equiv 0 \pmod{5^2}$$

Take  $a_2 = -1 + t \cdot 5$ , where  $t f'(-1) \equiv \frac{-f(-1)}{5} \pmod{5}$ .

$$f'(x) = 3x^2 + 1, \quad f'(-1) = 3 + 1 \equiv 4 \pmod{5},$$

$$f(-1) = -\left(\frac{-57}{5}\right) \equiv 11 \pmod{5} \equiv 1 \pmod{5},$$

$$\therefore t \text{ is s.t. } 4t \equiv 1 \pmod{5}, \quad \text{let } t = -1.$$

$$a_2 = -1 + (-1) \cdot 5 = -6 \pmod{25}.$$