

**MATHEMATICS 350 FALL 2008 (SHATZ)**  
**Assignment V, November 3, 2008. Due November 17, 2008**

Beatrice admonishes Dante (Paradiso, Canto 28, l. 58-60):

“Se li tuoi diti non sono a tal nodo  
sufficienti, non è meraviglia:  
tanto, per non tentare, è fatto sodo!”

Dante admonishes himself (Paradiso, Canto 33, l. 133-136):

“Qual è l'geometra che tutto s'affige  
per misurar lo cerchio, e non ritrova,  
pensando, quel principio ond' elli indige,  
tal era io a quella vista nova.”

**A PROBLEMS (NOT TO BE HANDED IN).**

AI Suppose  $n$  is a given integer and consider  $\mathbf{Z}/n\mathbf{Z}$ . An integer  $r$  is a *generator* mod  $n$  when and only when all the powers of  $r$ , namely  $r^t$ , run over all of  $(\mathbf{Z}/n\mathbf{Z})^*$ . A generator need not exist mod  $n$ , but when  $n$  is a prime it does. Use this to show that when  $n$  is prime, then the integer

$$1^s + 2^s + \cdots + (n-1)^s$$

is congruent to either 0 or -1 mod  $n$  depending on the value of the integer  $s \geq 0$ . For which  $s$  is it 0, for which is it -1? Show further that if  $r$  is a generator mod  $m$  and if  $d|m$ , then  $r$  is also a generator mod  $d$ .

AII Continue the investigation of the problem above. Take an odd prime  $p$ , and prove that for all  $n \geq 0$

$$(1 + px)^{p^n} \equiv 1 + p^{n+1} \pmod{p^{n+2}}.$$

From this, show that if  $r$  is a generator mod  $p$ , then it is also a generator mod  $p^n$  if and only if  $p^2$  does not divide  $(r^{p-1} - 1)$ . Show that in any case (for a generator mod  $p$ ) either  $r$  or  $r + p$  is a generator mod  $p^n$ .

AIII Take an integer  $m > 1$  and a prime number  $q$ . Write  $r$  for the integer  $\text{ord}_q(m^m - 1)$  and assume  $r > 0$ . Now let  $h$  be the least positive integer satisfying  $m^h \equiv 1 \pmod{q}$ . Prove that  $r = \text{ord}_q(m^h - 1)$ . More generally, say that  $h|s$  and  $s|m$ , show that  $r = \text{ord}_q(m^s - 1)$ .

**B PROBLEMS (TO BE HANDED IN–GROUP WORK).**

BI Assume you know the Prime Number Theorem (PNT). On the basis of this knowledge, prove the following: Given any  $\epsilon > 0$ , there is an integer  $N$  (which will depend upon  $\epsilon$ ), so that for any real number,  $x > N$ , there is a prime number  $p$  that satisfies  $x < p \leq x(1 + \epsilon)$ . The corresponding statement that there is always a prime between  $x$  and  $2x$  was conjectured by Bertrand and proved by Chebychev in the mid-nineteenth century before your sharper statement above which uses the PNT (proved in 1898).

BII Let  $x \geq 2$  be a real number. Prove that

$$\prod_{p \leq x} p < 4^x.$$

(Suggestions: Of course, this is true for  $x$  between 2 and 3; so, show first that if you know it for  $x$  an odd integer  $\geq 3$  you will know it for all required  $x$ . Replace  $x$  by the odd integer  $n$  and do an induction on  $n$ . For this, look at  $\binom{n}{k}$  and pick an appropriate  $k$ .)

BIII a) Let's call an integer,  $n$ , *square free* if in its prime factorization all the primes occur with exponent 1. Now set  $\mu(n) = (-1)^r$  if  $n$  is square free with  $r$  prime factors, and set  $\mu(n) = 0$  (resp.  $= 1$ ) if  $n$  is not square free (resp. if  $n = 1$ ). It's easy to see that if  $a$  and  $b$  are relatively prime, then  $\mu(ab) = \mu(a)\mu(b)$ . Prove that  $\sum_{d|n} \mu(d)$  is 1 if  $n = 1$  and is 0 for all  $n > 1$ .

b) If  $K$  is a field, any solution in  $K$  to the equation  $X^m - 1 = 0$  is called an  $m^{\text{th}}$  root of unity in  $K$ . It is a *primitive*  $m^{\text{th}}$  root of unity when it is not an  $r^{\text{th}}$  root of unity for any  $r < m$ . Suppose our field  $K$  contains a primitive  $m^{\text{th}}$  root of unity, denote it  $\xi$ . (This is the case for  $K = \mathbf{C}$  for every  $m$ , it is the case for  $\mathbf{F}_5$  when  $m = 4$ , etc.) We denote by  $F_d(X)$  the product of the factors  $(X - \xi^t)$  for  $0 \leq t < m$  and  $t$  relatively prime to  $\frac{m}{d}$ . Show that the degree of  $F_d(X)$  is  $\Phi(d)$  and prove that

$$X^m - 1 = \prod_{d|m} F_d(X).$$

Deduce that

$$F_m(X) = \prod_{d|m} (X^{m/d} - 1)^{\mu(d)}.$$

c) Suppose our field  $K$  is as in b) above. Show that the sum of all the

primitive  $m^{\text{th}}$  roots of unity in  $K$  is  $\mu(m)$ . Explicitly, what does this say if  $K = \mathbf{F}_p$  and  $m = p - 1$ ?