Number Theory

(Math 281)
Final Exam
January 1999

Ali Nesin & Özlem Beyarslan

I. Recall that we proved in class that if p is an odd prime and n any integer, then $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic.

a. What is the order of $(\mathbb{Z}/p^n\mathbb{Z})^*$ if p is a prime?

b. Show that 2 is a generator of $(\mathbb{Z}/9\mathbb{Z})^*$, $(\mathbb{Z}/125\mathbb{Z})^*$.

c. Find an odd prime p such that 2 is not a generator of $(\mathbb{Z}/p\mathbb{Z})^*$.

d. Show that $(\mathbb{Z}/2\mathbb{Z})^*$ and $(\mathbb{Z}/4\mathbb{Z})^*$ are cyclic.

e. Show that $(\mathbb{Z}/8\mathbb{Z})^*$ is not cyclic.

f. Show that $(\mathbb{Z}/2^n\mathbb{Z})^*$ is cyclic if and only if $n = 0$, 1 or 2.

g. For what numbers m is $(\mathbb{Z}/m\mathbb{Z})^*$ cyclic?

II.

a. Is 4031 a square modulo 4013? (4013 is a prime and $4031 = 29 \times 139$).

b. For what primes p is 2 a square in the prime field $\mathbf{F}_p$?

III. Show that F_{p^m} is a subfield of F_{p^n} if and only if m divides n.

IV.

a. Let p be any odd prime. Show that every element of $\mathbf{F}_p$ is a square in the field F_{p^2}. (**Hint:** Up to isomorphism, there is only one field of a given finite cardinality).

b. Show that 2 is a square in the field F_{p^n} (p odd) iff either 2 is a square in $\mathbf{F}_p$ or n is even. (**Hint:** Use IVa and II).