Number Theory Homework #5

Prof. Zeev Rudnick

To be handed in by Monday, December 5, 2011.

---

1) Let $\mathbf{F}_2=\mathbf{Z}/2\mathbf{Z}$. Find representatives for the residue classes of $\mathbf{F}_2[x]$ modulo the polynomial f(x), and compute the multiplication table for the ring $\mathbf{F}_2[x]/(f(x))$, where

i) $f(x)= x + 1$ ii) $f(x) = x^2 + x + 1$ iii) $f(x) = x^2 + 1$

Which of these rings are fields ?

2) Let $\mathbf{F}_3=\mathbf{Z}/3\mathbf{Z}$. Show that there are infinitely irreducible polynomials P(x) in $\mathbf{F}_3[x]$ which satisfy $P(0) = -1$.

3) For an invertible residue a mod N, the order (סדר) of a mod N is the least integer $k\geq 1$ for which $a^k=1 \bmod N$. Find the order of 5 mod p for all primes $5 < p < 50$.

Course homepage: http://www.math.tau.ac.il/~rudnick/courses/int_numth.html