Number Theory Homework #4

Prof. Zeev Rudnick

To be handed in on Monday, December 5, 2016.

---

1) Let F_2=**Z**/2**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 **F** be a field. Show that there are infinitely many **monic** irreducible polynomials in **F**[x]. (A **monic** polynomial is of the form $\mathbf{1} \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_0$).

3) Let $\mathbf{F}_3$=**Z**/3**Z** be the field with 3 elements. Show that there are infinitely many **monic** irreducible polynomials $P(x) = x^n + a_{n-1}x^{n-1} + \cdots \in \mathbf{F}_3[x]$ such that $P(0) = -1$.

4) Find the last two digits in the decimal expansion of 3^{1123}. (For example the last two digits of 1729 are 29). Explain how to do the same for 3^n for any n.

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

Mailbox 085, first floor of Schreiber building

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