

MAT 311: Number Theory

Spring 2008

Solutions to HW4

1. Determine the number of solutions of the congruence $2x^3 + 5x^2 - 6x + 2 \equiv 0 \pmod{7}$.
By letting x run from 0 to 6 and computing the above expression $\pmod{7}$ we see that NO such x exists. \square
2. Find all roots of $1 + x + x^2 + \cdots + x^{p-2} \equiv 0 \pmod{p}$.
Since this polynomial divides $x^p - x$, it turns out that all of its roots are distinct. Thus it has precisely $p - 2$ (distinct) roots. Clearly $x = 0$ and $x = 1$ are not roots of the above congruence. Therefore the remaining $p - 2$ elements of \mathbb{Z}_p , namely $\{2, 3, \dots, p - 1\}$ are the roots we are looking for. \square
3. Find a non-constant polynomial in $\mathbb{Z}_p[x]$ with no roots in \mathbb{Z}_p .
One such polynomial would be $x^p - x$ as all elements of \mathbb{Z}_p satisfy $x^p \equiv x \pmod{p}$ by Fermat. \square
4. Expand $x(x - 1) \cdots (x - (p - 1)) \in \mathbb{Z}_p[x]$.
Observe that all elements of \mathbb{Z}_p constitute the roots of this polynomial. But by Theorem 2.29 of NZM, this implies that $x(x - 1) \cdots (x - (p - 1))$ is a factor of $x^p - x$ in $\mathbb{Z}_p[x]$. But both polynomials have the same degree ($= p$) and they are monic (i.e. the leading coefficients are 1), thus we must have $x(x - 1) \cdots (x - (p - 1)) = x^p - x$ in $\mathbb{Z}_p[x]$. \square