Elementary Number Theory

Problem Set 7

A selection of exercises on polynomials

Andrew Dong

Professor Ngo Bao Chau
Minh-Tam Trinh

December 4, 2015

Math 17500: Problem Set 7

1. Find the polynomial P $\in$ R[t] of smallest degree such that P(1) = -1, P(2) = 9 and P(3) = 10

Solution:

We have 3 points so this means that we take a polynomial of 2 degrees of the form $P(x) = ax^2 + bx + c$. We then plug in values P(1) = -1, P(2) = 9 and P(3) = 10 to obtain a system of equations. Solving this system of equations we get $a = -\frac{29}{2}, b = 10 + \frac{3*29}{2}, c = -11 - \frac{2*29}{2}$. Thus, the polynomial of smallest degree is $P(x) = -\frac{29}{2}x^2 + (10 + \frac{3*29}{2})x - 11 - \frac{2*29}{2}$.

2. Find P $\in$ C[t] of smallest degree such that P(1) = -1, P(i) = 9 and P(1 + i) = -10

Solution:

Again we have 3 points so we take a polynomial of 2 degrees of the form $P(x) = ax^2 + bx + c$. Plugging in values P(1) = - 1, P(i) = 9 and P(1 + i) = - 10 to obtain a system of equations. Solving this we get $P(x) = (-1 - \frac{28-20i}{1+i} - 4(28 - 20i))x^2 + (\frac{28-20i}{1+i})x + 4(28 - 20i)$.

3. Find the smallest positive integer n satisfying the congruences n $\equiv$ 1 mod 3, n $\equiv$ 3 mod 7 and n $\equiv$ 7 mod 13

Solution:

We write this as a system of congruence equations and since 3,7,13 are relatively coprime we apply Chinese Remainder Theorem. We end up with the equation $7 * 13 + 3 * 2 * 3 * 13 + 7 * 5 * 3 * 7 \bmod 3 * 7 * 13$ which results in the congruence equation 52 mod 273 which implies that 52 is the smallest positive integer n satisfying the congruence equations.

4. Find all irreducible polynomials of the form $t^2 + a$ in $F_{11}[t]$.

Solution:

We find irreducible polynomials of the form $t^2 + a$ by finding the quadratic residues modulo 11 and taking values that are quadratic nonresidues for a. An integer is a quadratic residue if it is congruent to a perfect square. Luckily we have the law of quadratic reciprocity to aid us, which states that for two odd prime numbers a and b, the Legendre symbol $\frac{a}{b} * \frac{b}{a} = (-1)^{\frac{a-1}{2} * \frac{b-1}{2}}$. Since b = 11 is an odd prime number, we just need to check 3, 5 and 7. By law of quadratic reciprocity, 3 is an QNR, 5 is a QR and 7 is an QNR. Thus, irreducible polynomials in F_{11} are $t^2 + 3$ and $t^2 + 7$.

5. Find the number of zeros in F_{13} of the polynomial $t^{1000} + t100 + 1$

Solution:

F_{13} is isomorphic to Z/12Z. Furthermore, 2 is a primitive root of F_{13}. This means that 2^0 mod 12 $\equiv 2^{12} \equiv 2^{24}$ and so on. We have that $t^{1000} \equiv t^{1000 \text{ mod } 12}$ mod 13 $\equiv t^4$ mod 13 $\equiv t^{100}$. Thus it follows that we just need to solve $2t^4 \equiv 12$ mod 13 which can be rewritten $t^4 \equiv 6$ mod 13 for which no solutions exist, which implies that there zeros.

6. Show that if gcd(n,p-1) = 1, then the polynomial $t^n - 1 \in F_p[t]$ has exactly one zero in F_p.

Solution:

Since we know the gcd, we can rewrite this as $t^n \equiv 1$ mod p which we can turn into an arithmetic function $n * f(t) \equiv 0$ mod (p-1). One solution is the case in which f(t) is the zero map. Then $f^{-1}(f(t)) = 1$. Now suppose that f(t) is not the zero map, that is it maps t to some integer. Now we use the fact that n and p - 1 are relatively prime, and claim that one of n or f(t) must be 0 in order to solve or congruence equation $n * f(t) \equiv 0$ mod (p-1). n cannot be zero here, so f(t) must be the zero map.

7. Show that if gcd(n,p-1) = 1, then the polynomial $t^n - a \in F_p[t]$, for any $a \in F_p$, has exactly one zero in F_p.

Solution:

Here we proceed similarly returning a congruence equation similar to that in 6 this time $n * f(t) \equiv f(a)$ mod (p-1). Since n and p-1 are relatively prime then n can be inverted to give the congruence equation $f(t) \equiv -n + f(a)$ mod (p-1). Previously we showed that for a = 1 and f(a) = 0 f(t) must be zero. Now suppose a $\neq$ 1. If f(a) = n then we have f(t) = 0. f(a) only equals n once in z/(p-1)Z.