HW2 Solutions Math1250 Spring 2014

Sec. 20

#2: Either 2, 6, 7 or 8. You can check for $a=2,6,7,8$ the smallest positive int. n s.t. $a^n \equiv 1 \pmod{11}$ is $n=10$, & hence $a, a^2, \cdots, a^{10} \equiv 1 \pmod{11}$ are distinct. For example: $2^0=1$, $2^1=2$, $2^2=4$, $2^3=8$, $2^4=5$, $2^5=10$, $2^6=9$, $2^7=7$, $2^8=3$, $2^9=6$, $2^{10}=1$. So as sets the powers of 2 (mod 11) coincide with $\mathbb{Z}_{11}^* = \{1, \cdots, 10\}$.

#29 We show $n^{37}-n$ is div. by each of the primes 37, 19, 13, 7, 3 and 2. By Fermat's Little Thm. we know $37 \mid n^{37}-n$. Suppose $19 \nmid n$ then we know $n^{18} \equiv 1 \pmod{19} \Rightarrow (n^{18})^2 = n^{36} \equiv 1 \pmod{19} \Rightarrow n^{37} \equiv n \pmod{19}$ i.e. $19 \mid n^{37}-n$. If $19 \mid n$ clearly $19 \mid n^{37}-n$. For rest of the primes i.e. 13, 7, 3 & 2 the argument is similar. (The point is that $36 = 37-1$ is a multiple of $13-1=12$, $7-1=6$, $3-1=2$ and $2-1=1$.)

Sec. 21

#13

We need only to take $T=\{a, a^2, a^3, \cdots\}$ in #12. If a is not a zero div. then $T=\{a, a^2, \cdots\}$ does not contain a zero div., and clearly is closed under multiplication. In fact from #12 it follows that not only $Q(R,T)$ has 1 but also $\underline{a}$ has multi. inverse in $Q(R,T)$.

(Let us briefly explain solution to #12: suppose $T \subset R$ is a subset which is closed under multiplication and does not have any zero divisors. Analogous to the construction of field of quotients consider $\{(x,y) \mid x \in R, y \in T\}$.

and let $Q(R,T)$ be the equiv. classes of the relation.

$(x,y) \sim (x',y')$ iff $xy' = yx'$, $x \in R$, $y \in T$

As before one checks that this is an equiv. relation, and $+$, $\times$ are defined exactly the same as for the field of fractions. Take $a \in T$ then one sees that the class $[(a,a)]$ is unity element because $\forall (x,y)$ we have:

$$(a,a)(x,y) = (ax, ay) = (xa, ya) \sim (x,y).$$
$$\| \quad (x,y)(a,a)$$

Sec. 22

31(c) As in the hint let:

$$f_i(x) = d_i (x-a_1) \cdots (x-a_{i-1})(x-a_{i+1}) \cdots (x-a_n).$$

We can choose value of d_i so that $f_i(a_i) = 1$, just put $d_i = ((a_i-a_1)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n))^{-1}$. Now suppose $\phi: F \longrightarrow F$ is a function and $\phi(a_i) = c_i \in F$ for any $i=1,\ldots,n$. (the c_i are arbitrary elements of the field F.) Now consider the polynomial

$f(x) = c_1 f_1(x) + \cdots + c_n f_n(x)$. It is easy to see for any i, $f(a_i) = c_i$ & hence f and ϕ coincide as functions. (In fact $f_1, \ldots, f_n$ constructed above are a "basis" for the vector space of all functions from $F \longrightarrow F$.)

Sec. 23

10 By inspection -1 is a zero of $f(x) = x^3 + 2x^2 + 2x + 1$ in $\mathbb{Z}_7[x]$. Executing the long division of polynomials we compute $f(x) = (x+1)(x^2+x+1)$.
$(x-(-1))$ ✓

By inspection 2 and 4 are zeros of x^2+x+1. Thus the factorization is $f(x)=(x+1)(x-4)(x-2)$.