Investigating Dynamic System: Assignment 2 #2

Due on December 13, 2023 at 3:10pm

Professor J Section A

V **U**

Problem 1

Show that any product of d consecutive integers is divisible by $d!$ (Suggestion: You know something that should make this easy.)

Proof. We need to show $d!$ divides $n(n+1)(n+2)\cdots(n+d-1)$ for all $n \in \mathbb{Z}$. We know that

$$\frac{n(n+1)\cdots(n+d-1)}{d!} = \frac{(n+d-1)!}{d!(n-1)!} = \binom{n+d-1}{d}$$

is an integer. Therefore, $d!$ divides $n(n+1)(n+2)\cdots(n+d-1)$ for all $n \in \mathbb{Z}$. $\square$

Problem 2

Let

$$f(t) = a_0 + a_1 t + \cdots + a_n t^n \in \mathbb{R}[t] \tag{1}$$

And let $c = 1/(a_n)^{1/n}$. Let

$$g(t) = f(ct - a_{n-1}/na_n) = b_0 + b_1 t + \cdots + b_{n-1}t^{n-1} + b_n t^n \tag{2}$$

(a) Compute b_0.

Solution

$$b_0 = g(0) = f(-a_{n-1}/na_n)$$

(b) Compute b_{n-1}

Solution

We need only to compute the coefficients of t^{n-1} in $g(t)$, which is the coefficient in

$$a_{n-1}\left(ct - \frac{a_{n-1}}{na_n}\right)^{n-1} + a_n\left(ct - \frac{a_{n-1}}{na_n}\right)^n \tag{3}$$

which is

$$\begin{aligned} a_{n-1}c^{n-1} - \binom{n}{n-1}(c)^{n-1}\left(\frac{a_{n-1}}{na_n}\right) &= a_{n-1}\frac{1}{a_n} \\ = a_{n-1}\left(\frac{a_{n-1}}{a_n} - 1\right)c^{n-1} \end{aligned}$$

(c) Compute b_n

Solution

We need only to compute the coefficients of t^n in $g(t)$, which is the coefficient in

$$a_n\left(ct - \frac{a_{n-1}}{na_n}\right)^n \tag{4}$$

which is

$$b_n = a_n c^n = a_n \cdot \frac{1}{a_n} = 1 \tag{5}$$

Problem 3

Let p be prime
(a) Show that:

$$\binom{p}{k} =_p 0 \text{ for } 0 < k < p$$

Proof. We know that

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

Since p is prime, p does not divide $k!$ or $(p-k)!$. Therefore, p divides $p!$ but not $\binom{p}{k}$. Hence, $\binom{p}{k} =_p 0$ for $0 < k < p$. □

(b) Let $a = 1 + bp^h$ with $h > 0$ and $\gcd(p, b) = 1$. Show that: $a^p = 1 + cp^{h+1}$ with $\gcd(p, c) = 1$, unless$p = 2$ and $h = 1$.

Solution

Proof. We know that

$$\begin{aligned} a^p = (1 + bp^h)^p &= \sum_{k=0}^{p} \binom{p}{k} (bp^h)^k \\ &= 1 + \sum_{k=1}^{p} \binom{p}{k} (bp^h)^k \\ &= 1 + \sum_{k=1}^{p} p \left(\binom{p}{k} \Big/ p \right) b^k p^{hk-h} \cdot p^h \\ &= 1 + p^{h+1} \sum_{k=1}^{p} \binom{p}{k} \Big/ p \cdot b^k p^{hk-h} \end{aligned}$$

□

Let

$$c = \sum_{k=1}^{p} \binom{p}{k} \Big/ p \cdot b^k p^{hk-h}$$

. Let's look at the first term of the sum. We know that

$$\binom{p}{1} \Big/ p \cdot b^k p^{h-h} = b^k$$

which is coprime to p since $\gcd(p, b) = 1$. Therefore, c is coprime to p. Hence, $\gcd(p, c) = 1$. □

(c) In the multiplicative group $(\mathbb{Z}_{p^e})^*$, $[1 + p]$ has order p^{e-1}.

Proof. Let $c_0 = 1$, we define c_n in the following way:

$$(1 + c_{n-1}p^{n-1})^p = 1 + c_n p^n$$

Thus,

$$(1 + p)^{p^{e-1}} = 1 + c_{e-1}p^e =_p 1$$

Conversely, if $h < e - 1$, then

$$(1 + c_h p^h)^p = 1 + c_{h+1}p^{h+1} \neq_p 1$$

Therefore, $[1 + p]$ has order p^{e-1}. □

(d) Prove that $(\mathbb{Z}_{p^e})^*$ is cyclic.

Proof. From (c), we know that $[1+p]$ has order p^{e-1} which is exactly the order of $(\mathbb{Z}_{p^e})^*$. Therefore, $(\mathbb{Z}_{p^e})^*$ is cyclic. $\square$

(e) For $e > 2$, prove that

$$(\mathbb{Z}_{2^e})^* \cong \{\pm 1\} \times \langle [5] \rangle$$

where $[5]$ has order 2^{e-2}.

Proof. From (b),

$$5^{p^h} = (1+2^2)^{p^h} = 1 + c2^{2+h}$$

Thus, $5^{p^h} =_p 1 \iff h = e-2$. Therefore, $[5]$ has order 2^{e-2}. Note that for $e > 2$ $5^{p^e} + 5^{p^e} = 2 \cdot 5^{p^e} \neq_{p^e} 0$. A homomorphism from $\{\pm 1\} \times \langle [5] \rangle$ to $(\mathbb{Z}_{2^e})^*$ can be given by: $(a, b) \mapsto ab$. This map is injective since $5^{p^e} + 5^{p^e} = 2 \cdot 5^{p^e} \neq_{p^e} 0$. This map is surjective since $|\{\pm 1\} \times \langle [5] \rangle| = |\mathbb{Z}_{p^e}| = 2^{e-1}$. Therefore,

$$(\mathbb{Z}_{2^e})^* \cong \{\pm 1\} \times \langle [5] \rangle$$

.

$\square$

Problem 4

Recall that a ring homomorphism $f : A \to A'$ satisfies

- $f(a+b) = f(a) + f(b)$
- $f(ab) = f(a)f(b)$
- $f(1) = 1$

A composition of ring homomorphisms is a ring homomorphism.
(a) Let p be a prime, Let $\mathbb{Z}_p \subseteq A$ be a commutative ring, so that $pa = 0$ for all $a \in A$. Show that $\phi : A \to A, \phi(a) = a^p$ is a ring homomorphism. And hence likewise for $\phi_e(a) = a^{p^e}$

Proof. We know that

$$\phi(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p = \phi(a) + \phi(b)$$

and

$$\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$$

and

$$\phi(1) = 1^p = 1$$

Therefore, ϕ is a ring homomorphism. Likewise, by induction, we assume that ϕ_{e-1} is a ring homomorphism. Then,

$$\phi_e(a+b) = (a+b)^{p^e} = \left(a^{p^{e-1}} + b^{e^{e-1}}\right)^p = a^{p^e} + b^{p^e} = \phi_e(a) + \phi_e(b)$$

And

$$\phi_e(ab) = (ab)^{p^e} = a^{p^e} b^{p^e} = \phi_e(a)\phi_e(b)$$

And

$$\phi_e(1) = 1^{p^e} = 1$$

Therefore, ϕ_e is a ring homomorphism. $\square$

(b) Show that, if $n = p^e m$, then:

$$\binom{n}{d} =_p 0 \text{ if } p^e \not| d \text{ and } \binom{n}{d} =_p \binom{m}{d'} \text{ if } d = p^e d'$$

Proof. Consider the expansion of $(t+1)^n$ in $\mathbb{Z}_{p^e}[t]$:

$$\sum_{d=0}^{n} \binom{n}{d} t^d = (1+t)^n = \left((1+t)^{p^e}\right)^m = (1+t^{p^e})^m = \sum_{d'=0}^{m} \binom{m}{d'} t^{p^e d'}$$

By comparing the coefficients of t^d on both sides, if $p^e \not| d$, then $\binom{n}{d} =_p 0$. If $d = p^e d'$, then $\binom{n}{d} =_p \binom{m}{d'}$. □

Problem 5

Let $f(t) \in \mathbb{C}[t]$. Show that if $f(\mathbb{Q}) \subseteq \mathbb{Q}$, then $f(t) \in \mathbb{Q}[t]$. (Suggestion: If $\deg(f) = d$, apply the proof of the Interpolation theorem to: $(0, f(0)), (1, f(1)), \cdots, (d, f(d))$).

Proof. By the Largrange Interpolation Theorem, we can express $f(t)$ as

$$f(t) = \sum_{i=0}^{d} \left(f(i) \prod_{j=0, j\neq i}^{d} \frac{t-j}{i-j} \right)$$

Since $f(\mathbb{Q}) \subseteq \mathbb{Q}$, we know that $f(i) \in \mathbb{Q}$ for all $i \in \mathbb{Z}$. The operations on the right hand side of the equation generate rational coefficients for $f(t)$. Therefore, $f(t) \in \mathbb{Q}[t]$. □