§20. #5 – $37^{49} \bmod 7$

$37 \equiv 2 \bmod 7$, so $37^{49} \equiv 2^{49} \bmod 7$

By Fermat, $2^6 \equiv 1 \bmod 7$, and

$49 = 6 \cdot 8 + 1$, so $2^{49} = (2^6)^8 \cdot 2 \equiv 1 \cdot 2$

$\equiv 2 \bmod 7$

---

§20 #11 $2x \equiv 6 \pmod 4$

$\iff 2x \equiv 2 \pmod 4$.

$\gcd(2,4) = 2$, $2 \mid 2$, so just

divide $\frac{2}{2} x \equiv \frac{2}{2} \bmod \frac{4}{2}$ or $x \equiv 1 \bmod 2$

$\iff x \equiv 1 \bmod 4$, $x \equiv 3 \bmod 4$

---

§20 #5 $36x \equiv 15 \pmod{24}$

$\gcd(36,24) = 12$ and $12 \nmid 15$

so no solutions

---

§22 #1 $f(x) = 4x - 5$

$g(x) = 2x^2 - 4x + 2$ in $\mathbb{Z}_8[x]$

$f(x) + g(x) = 2x^2 = 3 = [2]_8 x^2 + [0]_8 x + [5]_8$

$f(x) \cdot g(x) = 8x^3 - 10x^2 - 16x^2 + 20x + 8x - 10$

$= 8x^3 - 26x^2 + 28x - 10$

$= [0]_8 x^3 + [6]_8 x^2 + [4]_8 x + [6]_8$.

---

§22 #3 $f(x) = 2x^2 + 3x + 4$

$g(x) = 3x^2 - 2x + 3$

$f(x) + g(x) = 5x^2 + 5x + 7$

$= [5]_6 x^2 + [5]_6 x + [1]_6$

in $(\mathbb{Z}/6\mathbb{Z})[x]$

$f(x) g(x) = 6x^4 + 13x^3 + 24x^2 + 17x + 12$

reduce mod 6

$[0]_6 x^4 + [1]_6 x^3 + [0]_6 x^2 + [5]_6 x + [0]_6$

or $x^3 + 5x$

---

#16 – §18-14

Suppose $R$ is a commutative ring

$a$ is idempotent if $a^2 = a$.

Suppose $a$ and $b$ are idempotent.

Then $(ab)^2 = ab \cdot ab = aa \cdot bb$

$= a^2 b^2 = ab$, so $ab$ is idempotent.

b. If $(r,s) \in \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$,

Then $(r,s)^2 = (r^2, s^2)$, so $(r,s)$

is idempotent $\iff r = r^2$ (in $\mathbb{Z}/6\mathbb{Z}$)

and $s = s^2$ (in $\mathbb{Z}/12\mathbb{Z}$)

| mod 6 | | mod 12 | | | |
|---|---|---|---|---|---|
| 0 | 0 ← | → 0 | 0 | 6 | 36 |
| 1 | 1 ← | 1 | 1 | 7 | 49 |
| 2 | 4 | 2 | 4 | 8 | 64 |
| 3 | 9 ← | 3 | 9 | 9 | 81 ← |
| 4 | 16 | → 4 | 16 | 10 | 100 |
| 5 | 25 | 5 | 25 | 11 | 121 |

$r \in \{0,1,3,4\}$ $\quad s \in \{0,1,4,9\}$

$\{0,1,3,4\} \times \{0,1,4,9\}$.

---

Math 417
HW 9
Due 4/12/19

If b.

12. $22x \equiv 5 \bmod 15$

$\iff 7x \equiv 5 \bmod 15$

$7 \cdot 13 = 91 \equiv 1 \bmod 15$, so $13 = 7^{-1}$

$13 \cdot 7x \equiv 13 \cdot 5 \bmod 15$

$91x \equiv 65 \bmod 15 \iff x \equiv 5 \bmod 15$

(or use Chinese Remainder Theorem

on $7x \equiv 5 \bmod 3$, $7x \equiv 5 \bmod 5$.

14. $45x \equiv 15 \bmod 24$ $\quad \gcd(r,s) = 1$.

$\gcd(45,24) = 3$; $45 = 3 \cdot 15$, $24 = 3 \cdot 8$

$\iff 15x \equiv 5 \bmod 8$

$15 \equiv 7$ $\quad 7x \equiv 5 \bmod 8$ $\quad 7 \equiv -1 \bmod 8$.

$7 \cdot 7 = 49 \equiv 1 \bmod 8$, so $7^{-1} = 7 \bmod 8$.

$7 \cdot (7x) \equiv 7 \cdot 5 \bmod 8$

$49x \equiv 35 \bmod 8$

$x \equiv 3 \bmod 8$

or $x \equiv 3, 11, 19 \bmod 24$

#2. $\phi: \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ is a ring homomorphism

$\phi([1]_4) = [a]_6$

We must have $\phi([4]_4) = [4a]_6 = [0]_6$

So $4a \equiv 0 \bmod 6$

$\Rightarrow a \equiv 0, 3 \bmod 6$

$\phi([1]_4^2) = \phi([1]_4)$

So $[a^2]_6 = [a]_6$.

$a=0$ ✓ $a=3$ $9 \equiv 3 \bmod 6$

So two cases.

1) $a=0$. $\phi([2]_4) = \phi([3]_4) = [0]_6$

2. $a=3$ $\phi([1]_4) = [3]_6$,

$\phi([2]_4) = [0]_6$, $\phi([3]_4) = [3]_6$.

---

#3 $g(x) = x^2 + x$ in $\mathbb{Z}/6\mathbb{Z})[x]$

$0^2 + 0 = 0 \equiv 0$

$2^2 + 2 = 6 \equiv 0$

$3^2 + 3 = 12 \equiv 0$

$5^2 + 5 = 30 \equiv 0$ mod 6

$g(x) = x(x+1) = x(x-5)$

what about $(x-2)(x-3)$

$= (x+4)(x+3) = x^2 + 7x + 12$

$\equiv x^2 + x$ in $\mathbb{Z}/6\mathbb{Z})[x]$

So $g(x) = x(x+1) = (x+3)(x+4)$

in $\mathbb{Z}/6\mathbb{Z})[x]$.

---

#4. As seen in class on Wed (see webpage if you want here), if $\gcd(a,10) = 1$, then $a^{20} \equiv 1 \bmod 100$.

$\gcd(3,10) = 1$, so $3^{20} \equiv 1 \bmod 100$

$3^{63} = (3^{20})^3 \cdot 3^3 \equiv 1^3 \cdot 27 \bmod 100$

Last 2 digits are "27".

Doesn't work for 2!

$2^{63} \bmod 4 = 0$ because $2^2 | 2^{63}$!

But, $\gcd(2,25) = 1$, so $2^{20} \equiv 1 \bmod 25$

($\phi(25) = 20$) And

$2^{63} = (2^{20})^3 \cdot (2^1)^3 \equiv 1^3 \cdot 2^3 \equiv 8 \bmod 25$

So $2^{63} \equiv 0 \bmod 4$ $2^{63} \equiv 8 \bmod 25$.

Suppose $x \equiv 0 \bmod 4$, $x \equiv 8 \bmod 25$

$x = 25u + 8$ from the second, so

$25u + 8 \equiv 0 \bmod 4$; $u + 0 \equiv 0 \bmod 4$

$u \equiv 0 \bmod 4$, $u = 4v$, So $x = 25 \cdot 4v + 8$

$v = 8 + 100v \equiv 8 \bmod 100$ and the last 2 digits are "08"

Mathematica tells me:

$3^{63} = 114\ldots427$

$2^{63} = 9223\ldots808$ ✓

---

#5 §22-27

a. $D(a_0 + a_1 x + \cdots + a_n x^n) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$

R is a Field of characteristic zero

a) $D(f+g) = D(f) + D(g)$?

$f = a_0 + a_1 x + \cdots + a_n x^n$

$g = b_0 + b_1 x + \cdots + b_m x^m$.

$\Rightarrow f+g = (a_0 + b_0) + (a_1 + b_1)x + \cdots$

$D(f) = a_1 + 2a_2 x + \cdots$

$D(g) = b_1 + 2b_2 x + \cdots$

$D(f+g) = a_1 + b_1 + (2a_2 + 2b_2)x + \cdots$

yes, they are equal

$D(fg) = D(f)D(g)$? No! $D(x) = 1$

$D(x) = 1$, $D(x \cdot x) = D(x^2) = 2x$!

5b $\ker(D) = \{f \in F[x] : D(f) = 0\}$

If $a_1 + 2a_2x + \cdots + na_nx^{n-1} = 0$ ($F$ has characteristic 0)

then $a_1 = a_2 = \cdots = a_n = 0$.

So $f \in \ker(D) \iff f = a_0$

ie, the constants!

5c Claim that $\text{Im}(D) = F[x]$

If $f(x) = a_0 + a_1x + \cdots + a_nx^n$,

then $D(g) = f$ if

$$g = a_0x + \frac{a_1}{2}x^2 + \cdots + \frac{a_n}{n+1}x^{n+1}.$$

Details you won't worry about

If $F$ is a field, $1 \in F$

so $1 + 1 + \cdots + 1 = n \cdot 1 \in F$

Is this equal to $0_F$?

If so, then $(1 + 1 + \cdots + 1)x = 0_F$

ie, $nx = 0$ for any $x \in F$

ie $F$ has char. zero.

So $n \cdot 1_F \in F$, $n \cdot 1_F \neq 0$,

so $\frac{1}{n 1_F}$ is defined, call it $n$.

I don't expect you to talk about this!

---

6. mod 4

| $a$ | $a^2$ |
|---|---|
| 0 | 0 |
| 1 | 1 |
| 2 | 0 |
| 3 | 1 |

$m^2 \equiv 1 \bmod 4 \iff m \equiv 1, 3$.

$m^2 \equiv 1 \bmod 8 \iff m = 1, 3, 5, 7$.

$m^2 \equiv 1 \bmod 16 \iff m \equiv 1, 7, 9, 15$

by just calculating mod.

$m = 32$ The solutions are

$m = 1, 15, 17, 31$.

Suppose $x^2 \equiv 1 \bmod 2^r$, $r \geq 3$

Claim: There are 4 solns

$x \equiv 1, 2^{r-1} - 1, 2^{r-1} + 1, 2^r - 1 \bmod 2^r$.

$1^2 = 1$ $(2^{r-1} - 1)^2 = 2^{2r-2} - 2 \cdot 2^{r-1} + 1$

$= 2^{2r-2} - 2^r + 1 \equiv 1 \bmod 2^r$

and similarly for the others

Proof. $x^2 \equiv 1 \bmod 2^r \Rightarrow$

$2^r \mid (x-1)(x+1)$, so at least one of $x-1$, $x+1$ is even, so $x$ is odd, so $x-1$ and $x+1$ are both even

But.. $2^2$ cannot divide both $x-1$ and $x+1$, so either $2 \mid x-1$ and $2^{r-1} \mid x+1$ or $2 \mid x+1$ and $2^{r-1} \mid x-1$.

That is, $x \equiv -1 \bmod 2^{r-1}$ or $x \equiv 1 \bmod 2^{r-1}$

and these imply the answers above

---

Correction & Error from the Wrong Solution

§18-23 Describe all ring homomorphisms $\phi: \mathbb{Z} \to \mathbb{Z}$

~~$\phi(1) = 1$~~ $\phi(0) = 0$ is true for any ring homomorphism.

Let $\phi(1) = a$. Then by addition, $\phi(n) = na$ for $n \in \mathbb{N}$ and by inverses $\phi(n) = na$ for $n < 0$.

But $1^2 = 1$ so $\phi(1^2) = \phi(1)\phi(1)$

or $a^2 = a \Rightarrow a = 0$ or $1$.

$a = 0 \iff \phi(n) \equiv 0$ boring.

$a = 1 \iff \phi(n) = n$ identity