Staple!

Team B____

Sets and Logic
MHF3202 7860

Home-B

Prof. JLF King
Wednesday, 06Mar2024

Due **BoC, Wedn, 20Mar2024**, wATMP! **Print this problem-sheet**; it is the first page of your write-up, with the blanks filled in (handwritten). Write **DNE** if the object does not exist or the operation cannot be performed. NB: **DNE** $\neq \{\} \neq 0$. [Put ordinal, Team-# and sign Honor Code.]

B1: *Show no work.*

20 20 a A K-set Ω has $2^{[K^2]} - 2^{\frac{K[K+1]}{2}}$ **non-symmetric** binrels. Its number of **anti-symmetric** binrels is $2^K \cdot 3^{\binom{K}{2}}$

[**Note:** Do not confuse symmetric with reflexive. Be *careful* on this problem.]

Prelim. Binrel **A** is ***anti-symmetric*** if $\forall \alpha, \beta \in \Omega$: $[\alpha \mathbf{A} \beta \;\&\; \beta \mathbf{A} \alpha] \Rightarrow \alpha{=}\beta$. A binrel can be simultaneously *symm* and *anti-symm*; e.g, the *empty relation*.

The ***diagonal binrel*** has $\alpha \mathbf{D} \beta$ IFF $\alpha{=}\beta$. A binrel is *symm and anti-symm* IFF it is a subset of **D**. □

Counting: On Ω, there are $2^{[K^2]}$ binrels . For $\alpha,\beta \in \Omega$, there are $K[K{+}1]/2$ many sets $\{\alpha, \beta\}$. [This includes the $\alpha{=}\beta$ case]. Thus, there are $2^{K[K+1]/2}$ symm-binrels on Ω. Hence, $2^{[K^2]} - 2^{K[K+1]/2}$ counts the *non*-symm. binrels.

Fix **A**, an anti-symm binrel. Each of the K pairs (ω, ω) can either be in or out of **A**; whence 2^K possibilities.

The number of 2-sets $\{\alpha, \beta\}$ is $\binom{K}{2}$. For the two ordered pairs (α, β) and (β, α), there are $2{\cdot}2 = 4$ possibilities for membership in **A**. The only possibility *inconsistent* with anti-symmetry, is if *both* (α, β) and (β, α) lie in **A**.

As 3 of the possibilities *are* compatible with anti-symmetry, it follows that there are $3^{\binom{K}{2}}$ possbilities for those pairs off the diagonal. In consequence, there are $2^K \cdot 3^{\binom{K}{2}}$ anti-symmetric binrels. ♦

Addendum. Note $K^2 = K + 2\frac{K^2-K}{2} = K + 2\binom{K}{2}$, so $2^{[K^2]} = 2^K \cdot 2^{2\cdot\binom{K}{2}}$. Thus the # of non-symmetric binrels is

$$2^{K^2} - 2^{K[K+1]/2} = 2^K \cdot \left[2^{2\cdot\binom{K}{2}} - 2^{\binom{K}{2}}\right] = 2^K \cdot \left[4^{\binom{K}{2}} - 2^{\binom{K}{2}}\right].$$

For large K we expect that it is easier for a binrel to be non-symm than to be anti-symm. And indeed, the ratio is

!!: $$\frac{\mathsf{NonS}(K)}{\mathsf{AntiS}(K)} = \frac{4^{\binom{K}{2}} - 2^{\binom{K}{2}}}{3^{\binom{K}{2}}} \asymp \left[\frac{4}{3}\right]^{\binom{K}{2}}.$$

The rightmost term is the asymptotic growth rate as $K \nearrow \infty$.

15 20 b Sum $\binom{45}{19} + 2\binom{45}{20} + \binom{45}{21} = \binom{T}{B}$, where $T =$ 47 and $B =$ 21. Using the same idea,

$$\binom{32}{13} + 3\binom{32}{14} + 3\binom{32}{15} + \binom{32}{16} = \binom{\tau}{\beta},$$

where $\tau =$ 35 and $\beta =$ 16.

Soln: For natnums $N>K$, recall "*Pascal's identity*"

†: $$\binom{N}{K} + \binom{N}{K+1} = \binom{N+1}{K+1}.$$

Using (†) twice hands us

$$\binom{45}{19} + \binom{45}{20} + \binom{45}{20} + \binom{45}{21} = \binom{46}{20} + \binom{46}{21} = \binom{47}{21}.$$

For $N > K+1$, the argument above establishes

‡: $$\binom{N}{K} + 2\binom{N}{K+1} + \binom{N}{K+2} = \binom{N+2}{K+2}.$$

Using (‡) twice yields the 2nd-equality in the problem.

In identity $\binom{N}{K} = \binom{N}{K}$, *the coeff is* $\binom{0}{0}$.
The coeffs in Pascal's identity are $\binom{1}{0}, \binom{1}{1}$.
In the 1st-sum, the coefficients are $\binom{2}{0}, \binom{2}{1}, \binom{2}{2}$.
The coefficients in the 2nd-sum are $\binom{3}{0}, \binom{3}{1}, \binom{3}{2}, \binom{3}{3}$.

What generalization does this suggest?

20 On $\Omega := [1\,..\,29]\times[1\,..\,29]$, define binary-relation **C** by: (x,α) **C** (y,β) IFF $x\cdot\beta \equiv_{30} y\cdot\alpha$. Statement "*Relation* **C** *is an* ***equivalence relation***" is: T F

Crossmult Soln: Relation **C** is not transitive, due to $\mathbb{Z}_{30}$ having non-trivial zero-divisors. For a CEX, note $(5,15)$ **C** $(3,3)$ and $(3,3)$ **C** $(1,1)$, yet $(5,15)$ is not **C**-related to $(1,1)$.

What about $\mathbb{Z}$? On $\mathbb{Z}\times\mathbb{Z}_{\neq 0}$, define cross-multiply binrel $\sim$ by $(n_1,d_1)\sim(n_2,d_2)$ IFF $n_1d_2 = n_2d_1$.

To show $\sim$ transitive, suppose

1: $(A,\alpha)\sim(B,\beta)$ *and*

2: $(B,\beta)\sim(C,\gamma)$,

where α,β,γ are *non-zero*.

Multiplying $A\beta \overset{\text{from (1)}}{=\!=} B\alpha$ by γ, then reordering [mult. is commutative and associative], yields

1′: $$A\gamma\cdot\beta = B\gamma\cdot\alpha\,.$$

Relation (2) says $B\gamma = C\beta$. Plugging this equality into (1′) gives

$$A\gamma\cdot\beta = C\beta\cdot\alpha \overset{\text{note}}{=\!=} C\alpha\cdot\beta\,.$$

The KEY STEP: *Since β is non-zero* (*i,e, is not a zero-divisor*), we may cancel the β to conlude that $\boxed{A\gamma = C\alpha}$. I.e, $(A,\alpha)\sim(C,\gamma)$.

Defn. For posint M, let $\Omega := \Omega_{\mathsf{M}}$ comprise the set of pairs (α,β) with $\alpha,\beta\in[1\,..\,\mathsf{M})$. Let **C**:= $\mathbf{C}_{\mathsf{M}}$ be the *cross-multiply* mod-M binrel on $\Omega\times\Omega$.

A ***duo*** $\mathbf{p},\mathbf{q}\in\Omega\times\Omega$ [i.e, a *pair of pairs*] is an ***AW*** –an anti-witness– if $\mathbf{p}\mathbf{C}\mathbf{q}$ *and* $\forall s\in\Omega\times\Omega$: *Whenever s is* **C***-related to either* $\mathbf{p}$ *or* $\mathbf{q}$, *then s is related to both.* □

AW-problem. For each composite modulus M*:*

∗: *Characterize the set of AW-duos* $\langle\mathbf{p},\mathbf{q}\rangle$.

The trivial case is $\mathbf{p}=\mathbf{q}$.

The above proof gives another class of AW-duos: *Those duos satisfying both $d\perp\mathsf{M}$ and $d'\perp\mathsf{M}$, where* $\mathbf{p}=(n,d)$ *and* $\mathbf{q}=(n',d')$. □

20 20 d Suppose that $\prec$ is a total-order on set $\mathcal{S}$, and $<$ is total-order on set Ω, both strict. Define binrel $\ll$ on $\mathcal{S}\times\Omega$ by:

$$(b,\beta) \ll (c,\gamma)$$

IFF *Either* $b \prec c$ *or* $[b = c$ and $\beta < \gamma\,]$.

Then:

Relation $\ll$ *is a total-order.* (T) F

Suppose $\prec$ *and* $<$ *are each well-orders.*

Then $\ll$ *is a well-order.* (T) F

Total-order: Transitivity of $\ll$ is the main issue. Suppose pair $\boldsymbol{P}_0 \ll \boldsymbol{P}_1$ and $\boldsymbol{P}_1 \ll \boldsymbol{P}_2$, where $\boldsymbol{P}_k = (b_k, \beta_k)$.

If either $b_0 \prec b_1$ or $b_1 \prec b_2$, then $b_0 \prec b_2$ [by transitivity of $\prec$] whence $\boldsymbol{P}_0 \ll \boldsymbol{P}_2$.

So WLOG $b_0 = b_1 = b_2$. Consequently, both $\beta_0 < \beta_1$ and $\beta_1 < \beta_2$. [We only need that one inequality be strict, but both are.] The transitivity of $<$ now gives $\boldsymbol{P}_0 \ll \boldsymbol{P}_2$.

Well-order: Consider a non-empty subset $Q \subset \mathcal{S}\times\Omega$. Extracting the 1st-elt of each ordered-pair, the set

$$\left\{ b \in \mathcal{S} \;\middle|\; \exists \beta \text{ with } (b,\beta) \in Q \right\}$$

is non-void, hence has a $\prec$-minimum elt; call it $\boldsymbol{m}$.

Extracting 2nd-elements, the set

$$\left\{ \gamma \in \Omega \;\middle|\; (\boldsymbol{m},\gamma) \in Q \right\}$$

is non-void, so *it* has a $<$-minimum elt which we'll call $\boldsymbol{\mu}$.

The Upshot: Pair $(\boldsymbol{m},\boldsymbol{\mu})$ is the $\ll$-minimum element of subset Q.

Carefully Type *your two essays, double–spaced. I suggest* LaTeX.

B2: Recall *Rabbits and Lights* from the zoomester's beginning: To your right are lights $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3, \ldots$. Each light has a toggle button; Press&release: the light illuminates; P&R again, it is extinguished.

Off to your left is a queue of rabbits; so we have

$$\ldots \mathcal{R}_3\ \mathcal{R}_2\ \mathcal{R}_1 \quad \mathcal{L}_1\ \mathcal{L}_2\ \mathcal{L}_3\ \mathcal{L}_4, \ldots$$

All the lights are initially off. *If* rabbit-α (i.e, $\mathcal{R}_\alpha$) jumps, then he will hop on lights $\mathcal{L}_\alpha, \mathcal{L}_{2\alpha}, \mathcal{L}_{3\alpha}, \ldots$, turning them all on. If rabbit-β now jumps, he will change the state of lights β, 2β, $3\beta, \ldots$, turning some on, and some off.

A Map f. A (finite or infinite) set $\mathsf{R} = \{\alpha_1, \alpha_2, \ldots\}$ of rabbit-indices is an element of powerset $\boldsymbol{\mathcal{P}} := \mathcal{P}(\mathbb{Z}_+)$. After those rabbits jump, we have a (finite or infinite) set $\mathsf{L} = \{\beta_1, \beta_2, \beta_3, \ldots\}$ of indices of illuminated lights. Define $f{:}\boldsymbol{\mathcal{P}}{\to}\boldsymbol{\mathcal{P}}$ by $f(\mathsf{R}) := \mathsf{L}$.

Our first-day class showed [*involution argument, and re-argued using the divisor-count τ-fnc*] that $f(\mathbb{Z}_+)$ is the set $\{1, 4, 9, \ldots\}$ of squares. Evidently $f(\varnothing) = \varnothing$ and $f(\{1,2\}) = \text{Odds}$. □

Q1 For each of the following questions, produce *either* a CEX [counterexample] *or* a formal proof.

Is f injective? Is f surjective?

Bit-seq defns. View $\boldsymbol{\mathcal{P}}$ as $2^{\mathbb{Z}_+}$; the set of bit-seqs. The empty-set is $\vec{\mathbf{0}}$ and $011010100010\ldots$ is the set of primes. As we know, $f(\vec{\mathbf{1}}) = 1001000010\ldots$, the squares.

For $\vec{\mu},\vec{\nu} \in \boldsymbol{\mathcal{P}}$, let $\vec{\mu} \oplus \vec{\nu}$ be mod-2 bitwise addition (no carry). Automatically, $\vec{\mu} \oplus \vec{\mu} = \vec{\mathbf{0}}$. Hence $(\boldsymbol{\mathcal{P}}, \oplus, \vec{\mathbf{0}})$ is a *group*; indeed, a *topological group*, and each element is an involution.

Let $0^c = 1$ and $1^c = 0$. Then $\vec{\mu}^c := \vec{\mu} \oplus \vec{\mathbf{1}}$ is the bitwise complement of $\vec{\mu}$.

Use $\vec{\mu}\rfloor_n$ for bit-n in $\vec{\mu}$. Use $n \in \vec{\mu}$ to mean $\vec{\mu}\rfloor_n = 1$. □

Soln. Consider an f-fixed-point $\vec{\mu}$. FTSOC, suppose $\vec{\mu} \neq \vec{\mathbf{0}}$. Then there is a smallest $\boldsymbol{m}$ with $\vec{\mu}\rfloor_{\boldsymbol{m}} = 1$. CLAIM: $f(\vec{\mu})\rfloor_{2\boldsymbol{m}} \neq \vec{\mu}\rfloor_{2\boldsymbol{m}}$ (*Why? The smallest rabbit in $\vec{\mu}$ is $\mathcal{R}_{\boldsymbol{m}}$, so the only other $\vec{\mu}$-rabbit that could hit $\mathcal{L}_{2\boldsymbol{m}}$ is $\mathcal{R}_{2\boldsymbol{m}}$. Hence $\mathcal{L}_{2\boldsymbol{m}}$ is **off** IFF $\mathcal{R}_{2\boldsymbol{m}}$ is in $\vec{\mu}$.*). UPSHOT: The only f-fixed-pt is $\vec{\mathbf{0}}$.

Consider $\vec{\mu},\vec{\nu} \in \boldsymbol{\mathcal{P}}$ with $f(\vec{\mu}) = f(\vec{\nu})$. Then

$$\vec{\mathbf{0}} \;=\; f(\vec{\mu}) \oplus f(\vec{\nu}) \;=\; f(\vec{\mu} \oplus \vec{\nu})\,.$$

Hence $\vec{\mu} \oplus \vec{\nu} = \vec{\mathbf{0}}$, whence $\vec{\mu} = \vec{\nu}$. So: f is injective. ♦

ALT: *f is injective.* Consider distinct $\vec{\mu},\vec{\nu} \in \boldsymbol{\mathcal{P}}$.

At $\boldsymbol{m}$, the smallest index-of-disagreement, suppose $\vec{\mu}$ has 0 and $\vec{\nu}$ has 1. And, that rabbits $\vec{\mu}\rfloor_{[1\,..\,\boldsymbol{m})} \overset{\text{note}}{=\!=} \vec{\nu}\rfloor_{[1\,..\,\boldsymbol{m})}$ turn lamp-$\boldsymbol{m}$ off, 0. Then $f(\vec{\mu})$ will leave lamp-$\boldsymbol{m}$ OFF, whereas $f(\vec{\nu})$ has lamp-$\boldsymbol{m}$ ON. So $f(\vec{\mu}) \neq f(\vec{\nu})$ ♦

Q2 For $\mathsf{L} \in \text{Range}(f)$, give an algorithm to produce an R for which $f(\mathsf{R}) = \mathsf{L}$. If you program, can you implement your algorithm in computer code?

Q3 Produce a (*non-trivial*) commutative, associative binop $\$: \boldsymbol{\mathcal{P}} \times \boldsymbol{\mathcal{P}} \to \boldsymbol{\mathcal{P}}$ which satisfies

$$\forall \mathsf{R},\mathsf{R}' : \quad f(\mathsf{R}\ \$\ \mathsf{R}') \;=\; f(\mathsf{R})\ \$\ f(\mathsf{R}')\,.$$

What can you tell me about this binary operator?

X marks the spot. Viewing $\boldsymbol{\mathcal{P}}$-elts as *sets*, then symmetric-difference $\$:= \triangle$ fills the bill.

Viewing $\boldsymbol{\mathcal{P}}$-elts as *bit-sequences*, then $\$:= \oplus$, addition-mod-2, is the same operation. ♦

Q4 What are all the f–fixed-points; those rabbit-lists R with $f(\mathsf{R}) = \mathsf{R}$?

What can you say about the dynamics of f? —does it have periodic points of order 2? 3? . . . ?

What is $f\big(f(\mathbb{Z}_+)\big) \overset{\text{note}}{=\!=} f\big(\text{Squares}\big)$? (Conjecture? Computer simulation?)

B3: The ***Threeish-numbers*** comprise $\mathcal{T} := 1 + 3\mathbb{N}$. In terms of PoP-factorization $\mathsf{T} = p_1^{E_1} \cdot \ldots \cdot p_K^{E_K}$ [where $p_1 < \ldots < p_K$ are $\mathbb{Z}$-primes, and each E_j is a posint]:

i Give/prove an IFF-characterization for when $\mathsf{T} \in \mathcal{T}$.

ii Give/prove an IFF-char. of when T is Threeish-*irreducible*.

iii Give/prove an IFF-char. of when T is Threeish-*prime*.

iv Using theorem(s) from The Web, prove or disprove: "*There are ∞ly many Threeish-primes.*"

Soln. First, a recap of classwork:

1.1: *Example.* The set of ***Threeish-numbers*** is

$$\mathcal{T} := \{1, 4, 7, 10, \ldots\} = \{n \in \mathbb{Z}_+ \mid n \equiv_3 1\} .$$

Ok, so $\mathcal{T}$ is not a ring. But $\mathcal{T}$ is sealed under multiplication, has no ZDs, and the only $\mathcal{T}$-unit is 1; we can make sense of "$\mathcal{T}$-irreducible" and "$\mathcal{T}$-prime".

Factoring 100, these two Threeish-factorizations

$$4 \cdot 25 = 100 = 10 \cdot 10 ,$$

show that none of $4, 10, 25$ is Threeish-prime. Yet each *is* Threeish-irreducible. [This, as their only non-trivial $\mathbb{N}$-factorizations use non-Threeish numbers]. □

1.2: ?? Threeish conundrum. *Given a "target" $\mathsf{T} \in [2 \,..\, \infty)$, write its usual $\mathbb{N}$-prime factorization,*

1.3: $$\mathsf{T} = p_1^{E_1} \cdot p_2^{E_2} \cdot \ldots \cdot p_L^{E_L} ,$$

with $p_1, \ldots, p_L$ distinct, and each E_ℓ a posint.

In terms of (1.3), give an IFF-characterization of:

i: *When T is Threeishian.*

ii: *When T is Threeish-irreducible.*

iii: *When T is Threeish-prime.*

iv: *Are there ∞ly many Threeish-primes? –or any at all?* [*Hint:* Look up Dirichlet's thm on arith.-progressions.] ◊

Solved by: *Keven H.*, 2013t.

1.4: *Standing notation.* An odd integer k is "**3Pos**" if $k \equiv_3 +1$, and is **3Neg** if $k \equiv_3 -1$.

Henceforth, use "p" for 3Pos-primes, and use "q" for 3Neg-primes. □

1.5: ?? Prime vs. Irred Thm. *Using (1.4): Fix a $\mathsf{T} \nmid 3$, and factor this posint as*

1.6: $$\mathsf{T} = \underbrace{p_1^{C_1} \cdot p_2^{C_2} \cdots p_J^{C_J}}_{=P} \cdot \underbrace{q_1^{D_1} \cdot q_2^{D_2} \cdots q_K^{D_K}}_{=Q} ,$$

with each exponent a posint.

i: *Integer T is in $\mathcal{T}$ IFF $D_1 + \ldots + D_K$ is even.*

ii: *Our T is $\mathcal{T}$-irreducible IFF it has form either $\mathsf{T} = q\widehat{q}$ [where these two 3Neg-primes might be equal] or $\mathsf{T} = p$.*

iii: *Lastly, T is $\mathcal{T}$-prime IFF $\mathsf{T} = p$.*

Also, there are infinitely many $\mathcal{T}$-primes. ◊

Pf (i). Evidently $\mathsf{T} \equiv_3 1^{C_1+\ldots+C_J} \cdot [-1]^{D_1+\ldots+D_K}$, so T is Threeishian IFF $S := D_1 + \ldots + D_K$ is even. Henceforth, assume T is Threeish-irreducible in (1.6). ♦

Proof of (ii). Since $P \cdot Q$ must be a trivial Threeish-factoring of T, necessarily either $P = 1$ or $Q = 1$.

Case: $Q = 1$ Our T is a single $\mathbb{Z}$-prime, hence is certainly Threeish-prime.

Case: $P = 1$ So $S \geq 2$. Were $S \geq 4$ then we could Threeish-factor $\mathsf{T} \overset{\text{note}}{=\!=} Q$ as product of two of the q-primes, times the product of the remaining q-primes; *nope.* So T has form $\mathsf{T} = q\widehat{q}$, where these two 3Neg-primes could be equal. The only non-trivial $\mathbb{N}$-factorization is into non–Threeish-numbers. Hence

$q\widehat{q}$ is Threeish-irreducible. ♦

Proof of (iii). Easily, if T is Threeish-prime, then T is Threeish-irred. So WLOG, $\mathsf{T} = q\widehat{q}$.

To see that $q\widehat{q}$ is *not* Threeish-prime, consider 2,5,11, which are 3Neg-primes. At least one of them differs from both q and $\widehat{q}$; suppose 5 differs. Thus T divides neither $c := 5q$ nor $d := 5\widehat{q}$. Yet T divides $c \cdot d$. ♦

Proof of (iv). A special case of Dirichlet's thm on arithmetic progressions says $3\mathbb{N} + 1$ owns ∞ly many primes –which, we just showed, are precisely the Threeish-primes. ♦

Aside. An easy extension of Euclid's method of proof showing $|\text{Primes}| = \infty$, applies to show that arith.prog $3\mathbb{N} - 1$ has ∞ly many primes.

Unfortunately, this easy extension doesn't apply to $3\mathbb{N} + 1$; I don't know any simple argument for that arith.prog. □

B1:	___ ___ ___	135pts
B2:	___ ___ ___	100pts
B3:	___ ___	85pts
Total:	___ ___ ___	320pts

HONOR CODE: *"I have neither requested nor received help on this exam other than from my team-mates and my professor (or his colleague)."* *Name/Signature/Ord*

Ord: ⌊.....⌋⌊.⌋⌊.⌋

Ord: ⌊.....⌋⌊.⌋⌊.⌋

Ord: ⌊.....⌋⌊.⌋⌊.⌋