Number Sets. An expression such as $k \in \mathbb{N}$ (read as "k is an element of $\mathbb{N}$" or "k in $\mathbb{N}$") means that k is a natural number; a ***natnum***.

$\mathbb{N}$ = natural numbers = $\{0, 1, 2, \dots\}$.

$\mathbb{Z}$ = integers = $\{\dots, -2, -1, 0, 1, \dots\}$. For the set $\{1, 2, 3, \dots\}$ of positive integers, the ***posints***, use $\mathbb{Z}_+$. Use $\mathbb{Z}_-$ for the negative integers, the ***negints***.

$\mathbb{Q}$ = rational numbers = $\{\frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z}_+\}$. Use $\mathbb{Q}_+$ for the positive ***ratnums*** and $\mathbb{Q}_-$ for the negative ratnums.

$\mathbb{R}$ = reals. The ***posreals*** $\mathbb{R}_+$ and the ***negreals*** $\mathbb{R}_-$.

$\mathbb{C}$ = complex numbers, also called the ***complexes***.

For $\omega \in \mathbb{C}$, let "$\omega > 5$" mean "ω *is* ***real*** *and* $\omega > 5$". [Use the same convention for $\geqslant, <, \leqslant$, and also if 5 is replaced by any real number.]

An "***interval of integers***" $[b \,..\, c)$ means the intersection $[b, c) \cap \mathbb{Z}$; ditto for open and closed intervals. So $[e \,..\, 2\pi] = \{3, 4, 5, 6\} = [3 \,..\, 6] = (2 \,..\, 6]$. We allow b and c to be $\pm\infty$; so $(-\infty \,..\, -1]$ is $\mathbb{Z}_-$.

Floor function: $\lfloor \pi \rfloor = 3$, $\lfloor -\pi \rfloor = -4$. Ceiling fnc: $\lceil \pi \rceil = 4$. Absolute value: $|-6| = 6 = |6|$ and $|-5 + 2i| = \sqrt{29}$.

Mathematical objects. Seq: '*sequence*'. poly(s): '*polynomial(s)*'. irred: '*irreducible*'. Coeff: '*coefficient*' and var(s): '*variable(s)*' and parm(s): '*parameter(s)*'. Expr.: '*expression*'. Fnc: '*function*' (so ratfnc: means rational function, a ratio of polynomials). cty: '*continuity*'. cts: '*continuous*'. diff'able: '*differentiable*'. CoV: '*Change-of-Variable*'. CoI: '*Constant of Integration*'. LoI: '*Limit(s) of Integration*'. RoC: '*Radius of Convergence*'.

Soln: '*Solution*'. Thm: '*Theorem*'. Prop'n: '*Proposition*'. CEX: '*Counterexample*'. eqn: '*equation*'. RhS: '*RightHand Side*' of an eqn or inequality. LhS: '*left-hand side*'. Sqrt **or** Sqroot: '*square-root*', e.g, "the sqroot of 16 is 4". Ptn: '*partition*', *but* pt: '*point*', as in "a fixed-pt of a map".

FTC: '*Fund. Thm of Calculus*'. IVT: '*intermediate-Value Thm*'. MVT: '*Mean-Value Thm*'.

The ***logarithm*** fnc, defined for $x>0$, is $\log(x) := \int_1^x \frac{dv}{v}$. Its inverse-fnc is $\exp()$. For $x>0$, then, $\exp(\log(x)) = x = e^{\log(x)}$. For real t, naturally, $\log(\exp(t)) = t = \log(e^t)$. PolyExp: '*Polynomial-times-exponential*'. E.g, $F(t) := [3 + t^2] \cdot e^{4t}$ is a polyExp.

Phrases. WLOG: '*Without loss of generality*'. TFAE: '*The following are equivalent*'. ITOf: '*In Terms Of*'. OTForm: '*of the form*'. FTSOC: '*For the sake of contradiction*'. Use iff: '*if and only if*'.

IST: '*It Suffices to*' as in ISTShow, ISTExhibit.

Use w.r.t: '*with respect to*' and s.t: '*such that*'.

Latin: e.g: *exempli gratia*, '*for example*'. i.e: *id est*, '*that is*'. N.B: *Nota bene*, '*Note well*'. QED: *quod erat demonstrandum*, meaning "end of proof".

P1: Wed. 30 Jun With $M := 22$ and $\mathbf{J} := [0 \,..\, M)$, use *repeated-squaring* to compute $6^{1024} \equiv_M$ ⌊.....⌋ $\in \mathbf{J}$. Since 1033 equals $2^{10} + 2^3 + 2^0$, power $6^{1033} \equiv_M$ ⌊.....⌋ $\in \mathbf{J}$. [*Hint:* Compute with symm. residues, and use periodicity.]

RS Soln: The period is tiny, so this is quick.

```
% (repeated-squaring 6 1033 22 :symmod t)

 /--------------------- Mod 22 ----\
  N:      2^N |     Accum |   6^[2^N]
---+----------+-----------+-------------
  0:        1 |         1 |         6 <<
  1:        2 |         6 |        -8
  2:        4 |         6 |        -2
  3:        8 |         6 |         4 <<
  4:       16 |         2 |        -6
  5:       32 |         2 |        -8
  6:       64 |         2 |        -2
  7:      128 |         2 |         4
  8:      256 |         2 |        -6
  9:      512 |         2 |        -8
 10:     1024 |         2 |        -2 <<
All:     done |        -4 |
 \--------------------- Mod 22 ----/

 So  6^{1033}  is mod-22 congruent
 to the product of the << marked values.
 Their mod-22 product is -4.
```

I.e: $6^{1024} \equiv_M -2 \equiv_M 20$. And $6^{1033} \equiv_M -4 \equiv_M 18$.

P2: Fri. 01 Feb LBolt: $\text{GCD}(70, 42) = \_\_\_\_ \cdot 70 + \_\_\_\_ \cdot 42$.

So (LBolt again) $G := \text{GCD}(70, 42, 60) = \_\_\_\_$ and $\_\_\_\_ \cdot 70 + \_\_\_\_ \cdot 42 + \_\_\_\_ \cdot 60 = G$.

P3: Wed. 06 Feb Carmichael fnc $\boldsymbol{\lambda}(385 \cdot 29 \cdot 43) = 2^A \cdot 3^B \cdot 5^C \cdot 7^D \cdot 11^E$ where $A = \_\_\_\_$, $B = \_\_\_\_$, $C = \_\_\_\_$, $D = \_\_\_\_$, $E = \_\_\_\_$.

Good Carma! Our $K := 385 \cdot 29 \cdot 43$ factors as $K = 5 \cdot 7 \cdot 11 \cdot 29 \cdot 43$. So $\Phi(K)$ is gp-isomorphic to $\text{Cyc}_{2^2} \times \text{Cyc}_{2\cdot 3} \times \text{Cyc}_{2\cdot 5} \times \text{Cyc}_{2^2\cdot 7} \times \text{Cyc}_{2\cdot 3\cdot 7}$. The product of the group-orders is $\boldsymbol{\varphi}(K) = 2^7 \cdot 3^2 \cdot 5^1 \cdot 7^2$.

All the groups are cyclic, so the exponent of the product group is simply the LCM of the group-orders. Hence $\boldsymbol{\lambda}(K) = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^0 = 420$.

[Were $K \nmid 4$, we'd recall that $\Phi(2^{N+2}) \overset{\text{gp}}{\cong} \text{Cyc}_2 \times \text{Cyc}_{2^N}$.]

P4: Fri. 08 Feb *Magic integers* G_1, G_2, G_3, each in $[0\,..\,330)$, are such that the $g{:}\mathbb{Z}_5{\times}\mathbb{Z}_6{\times}\mathbb{Z}_{11}{\hookrightarrow}\mathbb{Z}_{330}$ mapping is a ring-isomorphism, where

$$g\big((z_1, z_2, z_3)\big) \;:=\; \Big\langle z_1 G_1 + z_2 G_2 + z_3 G_3 \Big\rangle_{330}\,.$$

Then $G_3{=}$ ⌊ . . . . . ⌋ $\in [0\,..\,330)$. [Reduced product is $\vec{\mathbf{R}} = (66, 55, 30)$.]

Magic: Triple $(5, 6, 11)$ *is* pairwise-cop, so CRT applies. Recall: R_3 *times* $[\frac{1}{R_3}$ mod-$M_3]$ *. . . is Magic!* Now $30 \equiv_{11} -3$. And

```
  n:   r_n   q_n   t_n
/--------------------\
  0:    11    --     0
  1:    -3    -4     1
  2:    -1     3     4
\--------------------/
```

So -4 is a mod-11 recip of 30. With $\equiv$ meaning $\equiv_{330}$,

$$G_3 \;\equiv\; R \cdot \langle 1/R \rangle_M \;\equiv\; 30 \cdot [-4] \;\equiv\; 210\,.$$

Also: *"Element $g\big((6, 11, 5)\big)$ is a zero-divisor in $\mathbb{Z}_{330}$."* (Circle) *T* (F)

Zero-division? Each of $6, 11, 5$ is a unit w.r.t the corr. modulus, so tuple $(6, 11, 5)$ is a unit in the product-ring.

Aside: Curious about $g\big((6, 11, 5)\big)$? The magic tuple is $\vec{\mathbf{G}} = (66, 55, 210)$. We *could* compute

$$g\big((6, 11, 5)\big) \equiv [6 \cdot 66] + [11 \cdot 55] + [5 \cdot 210] \equiv 71\,.$$

Faster. . . is to reduce first, noting

$$(6, 11, 5) \quad =_{\mathbb{Z}_5 \times \mathbb{Z}_6 \times \mathbb{Z}_{11}} = \quad (1, -1, 5)\,.$$

So $g\big((6, 11, 5)\big)$ equals

$$g\big((1, -1, 5)\big) \equiv 66 - 55 + [5 \cdot 210] \equiv 71\,.$$

Reciprocals via CRT. To compute the $\mathbb{Z}_{330}$-recip of 71, we need but compute the $\mathbb{Z}_5{\times}\mathbb{Z}_6{\times}\mathbb{Z}_{11}$-recip of $(1, -1, 5)$; evidently $(1, -1, -2)$. And $g\big((1, -1, -2)\big) \equiv -79$.

The pre-CRT way is

```
% (lightning 330 71)

  n:   r_n   q_n   t_n
/--------------------\
  0:   330    --     0
  1:    71     4     1
  2:    46     1    -4
  3:    25     1     5
  4:    21     1    -9
  5:     4     5    14
  6:     1     4   -79
  7:     0 Infty   330
\--------------------/
```

P5: Mon. 11 Feb TMWFIt, 8 is a mod-125 primroot, since its mult-order (mod 125) is 100 $\overset{\text{note}}{=\!=}$ $\varphi(125)$. Use the CRT-isomorphism to compute the corresponding mod-250 primroot $R =$ $\in [0\,..\,250)$.

Primroots: Ring-iso $g\colon \mathbb{Z}_2\times\mathbb{Z}_{125} \hookrightarrow\!\!\!\!\rightarrow \mathbb{Z}_{250}$, engenders group-iso $g\colon \Phi_2\times\Phi_{125} \hookrightarrow \Phi_{250}$, whence $R = g\big((1,8)\big)$.

With moduli $M_1 := 2$ and $M_2 := 125$, guessing (or LBolt) provides $1{\cdot}M_2 + [\text{-}62]{\cdot}M_1 = 1$, giving magic $G_1 := 1{\cdot}M_2 = 125$ and $G_2 := [\text{-}62]{\cdot}M_1 = \text{-}124$.

Thus $g\big((1,8)\big)$ equals

$$1{\cdot}G_1 + 8{\cdot}G_2 = \text{-}867 \equiv_{250} 133\,.$$

Check: $133 \equiv_2 1$ & $133 \equiv_{125} 8$. I.e $g^{-1}(133)=(1,8)$.

P6: ?? Wed. 13 Feb Solve some of the World's Problems.