

E7, Posting Race. The *standard ordering* of the first five primes is $\mathcal{S} := \llbracket 2, 3, 5, 7, 11 \rrbracket$. Here is a different *ordering*: $\mathcal{T} := \llbracket 7, 2, 11, 5, 3 \rrbracket$. There are $5! = 120$ orderings.

For $F \in \mathbb{Z}_+$ and an ordering \mathcal{U} , let \mathcal{U} -name(F) be its tuple of exponents w.r.t \mathcal{U} . E.g, $F := 3528360$ factors as $2^3 \cdot 3^6 \cdot 5^1 \cdot 7^0 \cdot 11^2$. So the std-name of F is

$$\mathcal{S}\text{-name}(F) = (3, 6, 1, 0, 2). \quad \text{In contrast,}$$

$$\mathcal{T}\text{-name}(F) = (0, 3, 2, 1, 6).$$

a Produce an ordering \mathcal{U} and posint N so that

$$\mathcal{U}\text{-name}(\varphi(N)) = \text{UF-zipcode} \stackrel{\text{note}}{=} (3, 2, 6, 1, 1),$$

OR else prove that no such $\langle \mathcal{U}, N \rangle$ pair exists.

b Either exhibit a posint K so that

$$\mathcal{S}\text{-name}(\varphi(K)) = \text{UF-zipcode}$$

OR else prove that no such K exists. □

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*.

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’. Col: ‘Constant of Integration’. Lol: ‘Limit(s) of Integration’.

Fnc: ‘function’ (so ratfnc: means rational function, a ratio of polynomials). cty: ‘continuity’. cts: ‘continuous’. diff’able: ‘differentiable’.

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 Sroot: ‘square-root’, e.g, “the sroot 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’. CoV: ‘Change-of-Variable’.

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’. QED: *quod erat demonstrandum*, meaning “end of proof”.

Q1: ^{Tue.}_{28 Jun} May lightning ⚡ strike this table! (I.e, please fill in.)

n	r_n	q_n	s_n	t_n
0	98	—	1	0
1	21		0	1
2				
3				
4				

So $\text{Gcd}(98, 21) = \dots = [\dots \cdot 98] + [\dots \cdot 21]$.

And $x = \dots \in [0..98)$ solves $\text{congr. } 21x \equiv_{98} 7$.

Q2: ^{Tue.}_{05 Jul} Mod $K := 51$, the recipr. $\langle \frac{1}{20} \rangle_K = \dots \in [0..K)$.

[Hint: ⚡] So $x = \dots \in [0..K)$ solves $5 - 20x \equiv_K 2$.

Q3: ^{Wed?}_{06 Jul} With $N := 19$, then $\varphi(N) = \dots$. Thus EFT (Euler-Fermat) says that $7^{3620} \equiv_N \dots \in [0..N)$.

Q4: ^{Fri.}_{08 Jul} Magic integers G_1, G_2, G_3 , each in $[0..330)$, are such that the $g: \mathbb{Z}_{11} \times \mathbb{Z}_5 \times \mathbb{Z}_6 \rightarrow \mathbb{Z}_{330}$ mapping is a ring-isomorphism, where

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

Then $G_3 = \underline{\hspace{2cm}} \in [0..330)$. Also: "Element $g((5, 6, 11))$ is a zero-divisor in \mathbb{Z}_{330} ." (Circle) $\quad T \quad F$

Q5: ^{Thu.}_{14 Jul} Consider the three congruences C1: $z \equiv_{21} 18$, C2: $z \equiv_{15} 3$, and C3: $z \equiv_{70} 53$. Let z_j be the *smallest natnum* [or *DNE*] satisfying (C1) \wedge (Cj). Then

$$z_2 = \underline{\hspace{2cm}}; \quad z_3 = \underline{\hspace{2cm}}.$$

Q6: ^{Fri.}_{15 Jul} With $K := 105$, ring \mathbb{Z}_K has $|\mathbb{ZD}_K| = \dots$
 and $|\mathbb{NQR}_K| = \dots$.

Q7: ^{Mon.}_{18 Jul} “Integer $49 \in \mathbb{QR}_{91}$ ” *T F* and “ $100 \in \mathbb{QR}_{121}$ ”
T F.

Value $K := 857$ is prime. So “ $2 \in \mathbb{QR}_K$ ” *T F*
 and “ $-8 \in \mathbb{QR}_K$ ”. *T F*

The prime decomposition of $L := 22673$ is $7 \cdot 41 \cdot 79$. So
 “ $2 \in \mathbb{QR}_L$ ”. *T F*

Q9: ^{Thu.}_{21 Jul} Three Jacobi symbols: Two blanks are immed.:
 $\left(\frac{4203}{2006}\right) = \dots$ $\left(\frac{4203}{99}\right) = \dots$ $\left(\frac{120}{7117}\right) = \dots$
 Convolution $[\mu \otimes \mu](12) = \dots$
 [This μ is the Möbius fnc.]

Oy! Just as with the Unfinished Symphony, here we have the Unbegin Microquiz. . . □

Q Nein: ^{Fri.}_{22 Jul}
 Integers $\mathbf{13} = 4 + 9$ and $\mathbf{17} = 1 + 16$ are SOTS. So
 posits $X = \dots$, $Y = \dots$ and $S = \dots$, $T = \dots$
 with $X < S < T < Y$, engender these SOTS decompositions:
 $X^2 + Y^2 = [\mathbf{13} \cdot \mathbf{17}] = S^2 + T^2$.
 With $N := 72$: $\varphi(N) = \dots$, $\text{Carm}(N) = \dots$.

QBonus: ^{Tue.}_{26 Jul} State the Quadratic Reciprocity thm, (with all of its hypotheses):

Legendre symbol $\left(\frac{7}{103}\right) = \dots$.

Q8: ^{Wed.}_{20 Jul} Suppose $x, y, N \in \mathbb{Z}_+$, with $x^2 + 2y^2 = N$ and $N \perp x$. Thus “Integer $-2 \in \mathbb{QR}_N$ ” is: *T F*
 Thus “Integer $+2 \in \mathbb{QR}_N$ ” is: *T F*

With $N \in \mathbb{Z}_+$, consider a $z \in \mathbb{QR}_N$ and a Bézout-pair (U, V) such that $zU + NV = 1$.

Then “ U is a mod- N square” is: *AT AF Nei*

QA: ^{Thu.}_{28 Jul} Polynomial $f(x) := x^2 - x - 22$ has \mathbb{Z}_2 -root $Y_1 = 0$.

This lifts to \mathbb{Z}_8 -root $Y_3 = \dots$. And f has a \mathbb{Z}_5 -root of $Z_1 = -1$, lifting to \mathbb{Z}_{25} -root $Z_2 = \dots$.
 Magic $G_1 = \dots$, $G_2 = \dots$ realize ring-iso $\mathbb{Z}_8 \times \mathbb{Z}_{25} \rightarrow \mathbb{Z}_{200}$, which maps (Y_3, Z_2) to \dots , a \mathbb{Z}_{200} -root of f .

QB: ^{Tue.}_{02 Aug} Since $221 = 13 \cdot 17$, then $221 = a^2 + b^2$ where $a \perp b$ and posints $a = \dots \leq b = \dots$.

Doubling, $442 = x^2 + y^2$, where $x \perp y$ are posints, and $x = \dots \leq y = \dots$.

QC: ^{Wed.}_{03j8 Aug} Solve *some* of the World's Problems, involving: *Proof of Fermat SOTS thm, multinomial coeff, finite geom-series, EFT, Wilson's (involution ideas), Stein's problem, Repeated-squaring, CRT, Fusion, Irreducibility/primeness (Chris numbers), compositeness techniques, QuadRecipr (QR, NQR), LST (4NEG, 4POS, 8FAR, N-RONO), JST, Melding (cop-SOTS), Carmichael fnc, Dirichlet convolution ($\mu, \varphi, Id, \delta, \tau, \sigma$, Liouville), Necklace counting, LCM Lemma, Primroot Thm, Prime-squared Thm, Primroot Lifting Thm, Struc.-of- $\Phi(2^N)$, Index-w.r.t-a-generator, Hensel's -and their Progeny, Relatives, and Groupies.*

QD: ^{Thu.}_{04j8 Aug} Solve two of the World's Problems.