

Number Sets. Expression $k \in \mathbb{N}$ [read as “ k is an element of \mathbb{N} ” or “ k in \mathbb{N} ”] means that k is a natural number; a **natnum**. Expression $\mathbb{N} \ni k$ [read as “ \mathbb{N} owns k ”] is a synonym for $k \in \mathbb{N}$.

\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 rationals and \mathbb{Q}_- for the negative rationals.

\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 $\geq, <, \leq$, 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}_- . And $[-\infty..-1]$, is $\{-\infty\} \cup \mathbb{Z}_-$.

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’. Col: ‘Constant of Integration’. Lol: ‘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 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’.

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, $[3 + t^2] \cdot e^{4t}$. PolyExp-sum: ‘Sum of polyexps’. E.g, $f(t) := 3te^{2t} + [t^2] \cdot e^t$ is a polyexp-sum.

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 $6^{1024} \equiv_M \dots \in \mathbf{J}$. Since 1033 equals $2^{10} + 2^3 + 2^0$, power $6^{1033} \equiv_M \dots \in \mathbf{J}$.
[Hint: Compute with symm. residues, and use periodicity.]

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

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

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

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

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

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

P5: ^{Mon.}_{11 Feb} TMWFIIt, 8 is a mod-125 primroot, since its mult-order (mod 125) is $100 \stackrel{\text{note}}{\equiv} \varphi(125)$. Use the CRT-isomorphism to compute the corresponding mod-250 prim-root $R = \dots \in [0..250)$.

P6: ^{Fri.}_{01 Mar} For prime $p = 59$, value -2 is a p -QR. $T \quad F$
[Hint: LST or LST+RS.]

P7: ^{Mon.}_{11 Mar} a Suppose $y \in \text{QR}_N$, where N is oddprime. You compute Bézout mults U and V st. $yU + NV = 1$. Then “ U is a mod- N square” is: $AT \quad AF \quad Nei$

b With $p := 323$, and $H := \frac{p-1}{2}$, note $66^H \equiv_p -2$. Thus p is \dots .

P8: ^{Mon.}_{08 Apr} De-Elias bit-string **0110100100001011000010**, writing it in form $\langle n_1 \rangle \langle n_2 \rangle \dots \langle n_L \rangle$ remaining bits:

.....

P9: ^{Wed.}_{17 Apr} Let $f(x) := x^2 - 4x - 2$, and $\mathbf{z}_1 := c_0 := 3$; so $f(\mathbf{z}_1) \equiv_5 0$. Note $f'(\mathbf{z}_1) = \dots \not\equiv_5 0$. Use Hensel's lem. to compute coefficients $c_j \in [0..5)$ [put them in the blanks, below]

$$\mathbf{z}_4 = c_0 \cdot 5^0 + \overbrace{\dots}^{\mathbf{z}_2} \cdot 5^1 + \underbrace{\dots}_{\mathbf{z}_3} \cdot 5^2 + \dots \cdot 5^3$$

so that natnums $\mathbf{z}_j := \sum_{i \in [0..j)} c_i 5^i$ satisfy

$$f(\mathbf{z}_j) \equiv 0 \pmod{5^j}, \quad \text{for } j = 2, 3, 4.$$

PA: *^{Mon.}_{22 Apr} Let $f(x) := x^2 - x - 17$, and $\mathbf{z}_1 := c_0 := 2$; so $f(\mathbf{z}_1) \equiv_5 0$. Note $f'(\mathbf{z}_1) = \not\equiv_5 0$. Use Hensel's lem. to compute coefficients $c_j \in [0..5)$ [put them in the blanks, below]

$$\mathbf{z}_4 = \underbrace{c_0 \cdot 5^0 + \overbrace{}^{\mathbf{z}_2} \cdot 5^1 + \underbrace{}_{\mathbf{z}_3} \cdot 5^2 + } \cdot 5^3$$

so that *natnums* $\mathbf{z}_j := \sum_{i \in [0..j)} c_i 5^i$ satisfy

$$f(\mathbf{z}_j) \equiv 0 \pmod{5^j}, \quad \text{for } j = 2, 3, 4.$$

This semester we studied Affine codes, Diffie-Hellman, El Gamal, RSA, LBolt, Chinese Remainder thm, Euler phi, Carmichael lambda, repeated squaring, Primitive roots, Legendre & Jacobi symbols, Quad reciprocity, Kraft-McMillan, expected coding-length, Huffman, Ziv-Lempel, Entropy, WLLN, Hamming codes, among other topics. T F

Henselling to fame and fortune: Lisp:
`(% (hensel 2 :p 5 :f (cree-poly 1 -1 -17) :EndExpon 3)`

Henselling over ring <InTeGeRs>, using prime P := 5.

Evaluate poly F(x) := x^2 + -1x + -17
 at z1 := 2. Happily, F(2) = -15 =P= 0,
 so let's lift z1, if possible.

Note F'(x) = 2x + -1.
 Hence F'(z1) =P= 3 is NOT mod-P zero. LBolt
 gives
`<1/3>_P = 2.`

The update rule [Newton's Method] is:

$$*: z_{j+1} == z_j - 2 * F(z_j) \pmod{5^{j+1}}.$$

Ratio R := [F(z_j) / 5^j] is an integer.
 Let c_j, modulo 5. Thus

$$**: z_{j+1} == z_j + [c_j * 5^j] \pmod{5^{j+1}}.$$

Iterating:

j:	5^j	z_j	F(z_j)	c_j
1:	5	2	-15	1
2:	25	7	25	3
3:	125	82	6625	4

Note that $F(82) = 6625 = 1000 \cdot 6 + 625$. So

$$\frac{F(82)}{125} = [8 \cdot 6] + 5 \equiv_5 [-2 \cdot 1] + 0.$$

Hence $c_3 \equiv -1 \cdot 2 \cdot -2 \equiv 4$.