

Z1: ^{Wed.}_{30 Jan} a LBolt gives $G := \text{Gcd}(1533, 413) = \dots$. And $1533S + 413T = G$, where $S = \dots$ & $T = \dots$ are integers.

b Euler $\varphi(121000) = \dots$. Express your answer as a product $p_1^{e_1} \cdot p_2^{e_2} \dots$ of primes to posit powers, with $p_1 < p_2 < \dots$.

Z2: ^{Mon.}_{11 Feb} *Magic integers* $G_1 = \dots$, $G_2 = \dots$, $G_3 = \dots$, each in $(-165..165]$, are st. mapping $g: \mathbb{Z}_6 \times \mathbb{Z}_5 \times \mathbb{Z}_{11} \rightarrow \mathbb{Z}_{330}$ is a ring-isomorphism, where

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

Verify for your map: $g((1, 1, 1)) = 1$ and $[5 \cdot 11] \bullet G_1$ and analogously for G_2 and G_3 .

Z3: ^{Wed.}_{13 Feb} With $A := 13$, $B := 15$, $P := A \cdot B = 195$, let \mathbf{J} be $[-97..97]$. There is a ring-iso $F: \mathbb{Z}_A \times \mathbb{Z}_B \rightarrow \mathbb{Z}_P$ sending (α, β) to $\langle G\alpha + H\beta \rangle_P$, using magic numbers

$G = \dots \in \mathbf{J}$ and $H = \dots \in \mathbf{J}$. A

mod- P root of poly $h(x) := 15 \cdot [x + 10]^3 + 13 \cdot [x - 2]$ is $(\dots, \dots) \xrightarrow{F} \dots \in \mathbf{J}$.

Z4: ^{Mon.}_{18 Feb} Consider the four congruences C1: $z \equiv_8 1$, C2: $z \equiv_{18} 15$, C3: $z \equiv_{21} 18$ and C4: $z \equiv_{10} 3$. Let z_j be the *smallest natnum* satisfying (C1) $\wedge \dots \wedge$ (Cj). Then

$z_2 = \dots$; $z_3 = \dots$; $z_4 = \dots$.
 $(z_1 = 1), \quad z_2 = 33, \quad z_3 = 249, \quad z_4 = 753.$

Z5: ^{Wed.}_{27 Feb} Alice's RSA code has modulus is $M = 143$, and encryption exponent $\mathbf{E} := 37$, both public. Bob has a message that can be interpreted as a number β in $[0..M)$. Since Alice knows the secret factorization $M = p \cdot q$ into primes, $p=13$, $q=11$, she can compute the decryption exponent $\mathbf{d} = \dots \in \mathbb{Z}_+$. Bob's encrypted message $\mu := \langle \beta^{\mathbf{E}} \rangle_M = 141$. Alice decrypts it to $\langle \mu^{\mathbf{d}} \rangle_M = \dots \in [0..M)$.

Bonus: ^{Fri.}_{01 Mar} i Prof. King wears bifocals, and cannot read small handwriting. Circle one: **True! Yes! Who?**

ii Modulo $Q := 72$, poly $h(x) := x^2 + 16x - 17$ has many roots.

Z6: ^{Mon.}_{18 Mar} Bits $\langle 2 \rangle 0 \langle 3 \rangle 1 \langle 4 \rangle 0 \langle 3 \rangle 0 \langle 6 \rangle 1 \langle 0 \rangle \langle 7 \rangle$ decode in Idx-form, e.g $\langle 7 \rangle 1 \langle 3 \rangle 1 \langle 9 \rangle 0 \dots \langle 3 \rangle 1 \langle 0 \rangle \langle 4 \rangle$, to

\dots . As 20 bits, it is \dots . Use *Ziv-Lempel* seeded with $\langle 0 \rangle = ''$, $\langle 1 \rangle = '1'$, and $\langle 2 \rangle = '0'$. Using our fivebit-code, the 20 bits decode to symbols \dots .

Z7: ^{Fri.}_{22 Mar} Bits $01001010100100001110001101101100111$ decode in Idx-form, e.g $\langle 7 \rangle 1 \langle 3 \rangle 1 \langle 9 \rangle 0 \dots \langle 3 \rangle 1 \langle 0 \rangle \langle 4 \rangle$, to

\dots . As 15 bits, it is \dots . Use *Ziv-Lempel* seeded with $\langle 0 \rangle = ''$, $\langle 1 \rangle = '1'$, and $\langle 2 \rangle = '0'$. Using our fivebit-code, the 15 bits decode to symbols \dots .

Z8: ^{Wed.}_{27 Mar} ? Using dictionary 0: ϵ , 1: "1", 2: "0", compute $\text{EnZiv}(11001010) = \dots$

in $\langle 7 \rangle 1 \langle 34 \rangle 0 \dots$ notation. In bits, $\text{EnZiv}(11001010)$ is \dots .

Z9: ^{Fri.}_{29 Mar} ? **Reduce the the World's Difficulties.**

§A Potential quiz problems

Some of these may eventually appear on quizzes/exams; naturally, with different data. (And some quiz problems may appear that are not here.) *Please write DNE in a blank if the described object does not exist or if the indicated operation cannot be performed.*

Phi1: $N := \varphi(100) = \dots$. So $\varphi(N) = \dots$.

EFT says that $3^{165} \equiv_N \dots \in [0..N)$. Hence (by EFT) last two digits of $7^{3^{165}}$ are \dots .

Phi2: Write $27^{2009} \equiv_7 \dots$ (i.e, working mod 7) and $9^{35} \equiv_7 \dots$, each as a value in $[0..7)$.

RS1: With $M := 22$ and $J := [0..M)$, use repeated-squaring to compute $6^{4096} \equiv_M \dots \in J$. Since 4101 equals $2^{12} + 2^2 + 2^0$, the power $6^{4101} \equiv_M \dots \in J$. [Hint: Compute with symm. residues, and use periodicity.]

CRT and Fusion problems. The fun stuff!

CRT1: With $A := 29$, $B := 20$, $P := A \cdot B = 580$, let \mathbf{J} be $(-290..290]$. There is a ring-iso $F: \mathbb{Z}_A \times \mathbb{Z}_B \rightarrow \mathbb{Z}_P$ sending (α, β) to $\langle G\alpha + H\beta \rangle_P$, using magic numbers $G = \dots \in \mathbf{J}$ and $H = \dots \in \mathbf{J}$. A mod- P root of poly $h(x) := 20 \cdot [x + 9]^3 + 29 \cdot [x - 4]$ is $(\dots, \dots) \xrightarrow{F} \dots \in \mathbf{J}$.

CRT2: i Show all steps, except the $\frac{1}{2}$ tables, to compute a magic tuple \mathbf{G} so that $g: \mathbb{Z}_5 \times \mathbb{Z}_6 \times \mathbb{Z}_7 \rightarrow \mathbb{Z}_{210}$ is a ring-isomorphism, where

$$g((z_1, z_2, z_3)) := \langle z_1 G_1 + z_2 G_2 + z_3 G_3 \rangle_{210}.$$

ii Consider poly $h(x) := [x - 2][x - 32][x - 8]$. Find all solutions to congruences $h(x) \equiv_M 0$, for $M = 5, 6, 7$, displaying the results in a nice table. (Do not show work for this step.)

Now use your ring-iso to compute all solns x to $h(x) \equiv_{210} 0$, displaying the results in a table which shows which 3tup each came from. There are (not counting multiplicities) $K := \dots$ many solns.

Explain your method well; then show one computation giving a root different (mod 210) from 2, 32, 8.

CRT3: 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 $z_2 = \dots$; $z_3 = \dots$.

CRT4: Consider the four congruences C1: $z \equiv_8 1$, C2: $z \equiv_{18} 15$, C3: $z \equiv_{21} 18$ and C4: $z \equiv_{10} 3$. Let z_j be the smallest natnum satisfying (C1) \wedge (Cj). Then $z_2 = \dots$; $z_3 = \dots$; $z_4 = \dots$.

CRT5: Let $f(x) := x^2 - 9x + 14$, and $N := 30425$ ^{note} $p \cdot 25$, where $p := 1217$ is prime. The number of solns $x \in [0..N)$ to $f(x) \equiv_N 0$ is $K = \dots$. A number $Z \in [0..N)$ such that $f(Z) \neq 0$ yet $f(Z) \equiv_N 0$ is \dots .

[Hint: Find solns mod- p and mod-25, then use CRT.]

Misc problems. For Miss Cellaneous.

Mod1: For a posint K , let \equiv mean \equiv_K . DEFN: Expression “ $x \equiv y$ ” means \dots .

Please prove: THM: For all $b, \beta, g, \gamma \in \mathbb{Z}$, if $b \equiv \beta$ and $g \equiv \gamma$ then $[b \cdot g] \equiv [\beta \cdot \gamma]$.

Orb1: Define $G: [1..12] \rightarrow \mathbb{N}$ where $G(n)$ is the number of letters in the n^{th} Gregorian month. So $G(2) = 8$, since the 2nd month is “February”. The only fixed-point of G is \dots . The set of posints k where $G^{\circ k}(12) = G^{\circ k}(7)$ is \dots .

mf1: Since $4800 = 2^6 \cdot 3^1 \cdot 5^2$, it has \dots many positive divisors. [Write ANS naturally as a product of integers.]

mf2: The divisor-sum $\sigma(1500) = \dots$. Express your answer a product $p_1^{e_1} \cdot p_2^{e_2} \cdot \dots$ of primes to posint powers, with $p_1 < p_2 < \dots$.

Cyc1: Applying the Floyd cycle-finding (Tortoise & Hare) to a finite orbit which has tail $T := 3$ and eventual-period $L := 4$, yields hitting time $H = \dots$.

Coding

cH1 Suppose the letters A F H M N U have frequencies $\frac{12}{170}, \frac{46}{170}, \frac{38}{170}, \frac{18}{170}, \frac{15}{170}, \frac{41}{170}$, respectively. Construct the unique Huffman prefix-code with these frequencies; at each coalescing, use 0 for the less-probable branch and 1 for the more-probable. Draw the Huffman tree (large!). Label the branches and leaves with bits and letters. The name HUFFMAN encodes to \dots .

Examining the tree, what kind of Being is HUFFMAN? Answering the question “What’re y’all?”, message 10100010101001110100110111010! decodes

to _____ !

cH2 The Huffman code with letter-probabilities

$$I: \frac{12}{66} \quad M: \frac{5}{66} \quad O: \frac{7}{66} \quad R: \frac{4}{66} \quad S: \frac{32}{66} \quad T: \frac{6}{66}$$

codes these to bitstrings: I: _____ M: _____

O: _____ R: _____ S: _____ T: _____

Bitstring 1101101110011001110 decodes to

_____, answering: "What is Big Moose's name?"

Essay1: Compute a Huffman code for these five symbols.

A: 4/27 _____

B: 1/27 _____

C: 14/27 _____

D: 2/27 _____

E: 6/27 _____

When coalescing, use "0" to go to the smaller-prob. word.

And MECL($\frac{4}{27}, \frac{1}{27}, \frac{14}{27}, \frac{2}{27}, \frac{6}{27}$)= _____ bits.

ii Give the example (with picture) from class of a minimum expected-length code which is **not** a Huffman code. Argue that your code is indeed of MECL, and is not Huffman.

iii State the Huffman Coding thm from class. Sketch a proof of it; just show the main ideas. (And pictures)

cE1 Bitstring "0001000101111111101101001", via the Elias code, decodes to _____,

a sequence of *natnums* [hint: gun-blip-blip], followed by noise-bits _____.

The natnum-sequence decodes to rune-string "_____".

Conv, Elias(84)= _____ (bitstring)

cZ1 Using dictionary 0: ϵ , 1: "1", 2: "0", compute EnZiv(11001010)= _____,

in $\langle 7 \rangle 1 \langle 34 \rangle 0 \dots$ notation. In bits, EnZiv(11001010) is _____.

cZ2 Bits 01001010100100001110001101101100111 decode in Idx-form, e.g $\langle 7 \rangle 1 \langle 3 \rangle 1 \langle 9 \rangle 0 \dots \langle 3 \rangle 1 \langle 0 \rangle \langle 4 \rangle$, to _____.

As 15 bits, it is _____.

Use Ziv-Lempel seeded with $\langle 0 \rangle = \text{''}$, $\langle 1 \rangle = \text{'1'}$, and $\langle 2 \rangle = \text{'0'}$. Using our fivebit-code, the 15 bits decode to symbols _____.

Playing with fields

C1 Blanks $\in \mathbb{R}$. So $\frac{1}{2+3i} = \frac{\text{_____}}{\text{_____}} + i \cdot \frac{\text{_____}}{\text{_____}}$.

Thus $\frac{7-2i}{2+3i} = \frac{\text{_____}}{\text{_____}} + i \cdot \frac{\text{_____}}{\text{_____}}$.

By the way, $|5-3i| = \sqrt{\text{_____}}$.

C2 In \mathbb{R} : $[1+i]^{86} = \left[\frac{\text{_____}}{\text{_____}} \right] + i \cdot \left[\frac{\text{_____}}{\text{_____}} \right]$.

[Hint: Multiplying complexes multiplies their moduli, and adds their angles. You may use sin and cos if you wish.]