

**Z1:** <sup>Wed.</sup><sub>30 Jan</sub> **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  $p_1^{e_1} \cdot p_2^{e_2} \cdot \dots$  of primes to posit powers, with  $p_1 < p_2 < \dots$ .

**Z2:** <sup>Mon.</sup><sub>11 Feb</sub> *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:** <sup>Wed.</sup><sub>13 Feb</sub> With  $A := 13$ ,  $B := 15$ ,  $U := A \cdot B = 195$ , let  $\mathbf{J}$  be  $[-97..97]$ . There is a ring-iso  $F: \mathbb{Z}_A \times \mathbb{Z}_B \rightarrow \mathbb{Z}_U$  sending  $(\alpha, \beta)$  to  $\langle G\alpha + H\beta \rangle_U$ , using magic numbers  $G = \dots \in \mathbf{J}$  and  $H = \dots \in \mathbf{J}$ . A mod- $U$  root of poly  $h(x) := 15 \cdot [x + 10]^3 + 13 \cdot [x - 2]$  is  $(\dots, \dots) \xrightarrow{F} \dots \in \mathbf{J}$ .

**Z4:** <sup>Mon.</sup><sub>18 Feb</sub> 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:** <sup>Wed.</sup><sub>27 Feb</sub> 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  $\beta$  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:** <sup>Fri.</sup><sub>01 Mar</sub>

**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:** <sup>Mon.</sup><sub>18 Mar</sub> 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

As 20 bits, it is

having used Ziv seeded with  $\langle 0 \rangle = ' '$ ,  $\langle 1 \rangle = '1'$ , and  $\langle 2 \rangle = '0'$ .

Employing our fivebit-code, the 20 bits decode to symbols

**Z7:** <sup>Fri.</sup><sub>22 Mar</sub> 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

having used Ziv seeded with  $\langle 0 \rangle = ' '$ ,  $\langle 1 \rangle = '1'$ , and  $\langle 2 \rangle = '0'$ .

Employing our fivebit-code, the 15 bits decode to symbols

**Z8:** <sup>Wed.</sup><sub>27 Mar</sub> ? Using dictionary 0:  $\epsilon$ , 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

**Z9:** <sup>Fri.</sup><sub>29 Mar</sub> ? 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.) 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  $A := 29$ ,  $B := 20$ ,  $U := A \cdot B = 580$ ,  
 let  $\mathbf{J}$  be  $(-290..290]$ . There is a ring-iso  $F: \mathbb{Z}_A \times \mathbb{Z}_B \rightarrow \mathbb{Z}_U$   
 sending  $(\alpha, \beta)$  to  $\langle G\alpha + H\beta \rangle_U$ , using magic numbers  
 $G = \dots \in \mathbf{J}$  and  $H = \dots \in \mathbf{J}$ . A  
 mod- $U$  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  
 $\langle h(x) \equiv_{210} 0 \rangle$ , displaying the results in a table which shows  
*which* 3tup each came from. There are (not counting multi-  
 plicities)  $K := \dots$  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  $N := 30425 \overset{\text{note}}{=} \rho \cdot 25$ ,  
 where  $\rho := 1217$  is prime. The *number* of solns  
 $x \in [0..N)$  to  $\langle f(x) \equiv_N 0 \rangle$  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- $\rho$  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  $G: [1..12] \circlearrowleft$  where  $G(n)$  is the number of  
 letters in the  $n^{\text{th}}$  Gregorian month. So  $G(2) = 8$ , since  
 the 2<sup>nd</sup> 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  $\dots$ .

[January, February, March, April, May, June, July, August, Septem-  
 ber, October, November, December]

**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  $\rho_1^{e_1} \cdot \rho_2^{e_2} \cdot \dots$  of primes to  
 posint powers, with  $\rho_1 < \rho_2 < \dots$ .

**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 frequen-  
 cies  $\frac{12}{170}, \frac{46}{170}, \frac{38}{170}, \frac{18}{170}, \frac{15}{170}, \frac{41}{170}$ , respectively. Construct  
 the unique Huffman prefix-code with these frequen-  
 cies; at each coalescing, use 0 for the less-probable  
 branch and 1 for the more-probable. **Draw** the Huff-  
 man 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:  $I: \dots$   $M: \dots$

$O: \dots$   $R: \dots$   $S: \dots$   $T: \dots$

Bitstring **1101101110011001110** decodes to

$\dots$ , 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  $MECL(\frac{4}{27}, \frac{1}{27}, \frac{14}{27}, \frac{2}{27}, \frac{6}{27}) = \dots$  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 "**000100010111111101101001**", via the Elias code, decodes to

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

$$\text{Conv, Elias}(84) = \dots \quad (\text{bitstring})$$

**cZ1** Using dictionary 0:  $\epsilon$ , 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

**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

having used Ziv seeded with  $\langle 0 \rangle = '0'$ ,  $\langle 1 \rangle = '1'$ , and  $\langle 2 \rangle = '0'$ .

Employing our fivebit-code, the 15 bits decode to symbols

### Playing with fields

**C1** Blanks  $\in \mathbb{R}$ . So  $\frac{1}{2+3i} = \dots + i \cdot [\dots]$ .

Thus  $\frac{7-2i}{2+3i} = \dots + i \cdot [\dots]$ .

By the way,  $|5-3i| = \dots$ .

**C2** Note  $[1+i]^{86} = [\dots] + i \cdot [\dots]$ .

[Hint: Multiplying complexes multiplies their moduli, and adds their angles.]