NT-Cryptography
MAT4930 *7554*

Quizzes Z 30Jan2013

Z1: Mon. 27 Jan a LBolt gives $G := \mathrm{Gcd}(1533, 413) =$ ⌞⌟. And $1533S + 413T = G$, where $S =$ ⌞.....⌟ & $T =$ ⌞.....⌟ are integers.

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

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

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

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

Z3: Wed. 13 Feb With $A := 13$, $B := 15$, $U := A{\cdot}B = 195$, let $\mathbf{J}$ be $[-97\,..\,97]$. There is a ring-iso $F: \mathbb{Z}_A \times \mathbb{Z}_B \to \mathbb{Z}_U$ sending (α, β) to $\langle G\alpha + H\beta \rangle_U$, using magic numbers $G =$ ⌞.....⌟ $\in \mathbf{J}$ and $H =$ ⌞.....⌟ $\in \mathbf{J}$. A mod-U root of poly $h(x) := 15{\cdot}[x+10]^3 + 13{\cdot}[x-2]$ is ⌞.....⌟, ⌞.....⌟ $\overset{F}{\mapsto}$ ⌞.....⌟ $\in \mathbf{J}$.

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) $\overset{\text{All}}{\ldots}$ (Cj). Then

$z_2 =$ ⌞.....⌟; $z_3 =$ ⌞.....⌟; $z_4 =$ ⌞.....⌟.
$(z_1 = 1)$, $z_2 = 33$, $z_3 = 249$, $z_4 = 753$.

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 $\mathbf{d} =$ ⌞.....⌟ $\in \mathbb{Z}_+$. Bob's encrypted message $\mu := \langle \beta^{\mathbf{E}} \rangle_M = 141$. Alice decrypts it to $\langle \mu^{\mathbf{d}} \rangle_M =$ ⌞.....⌟ $\in [0\,..\,M)$.

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 ⟨**2**⟩0 ⟨**3**⟩1 ⟨**4**⟩0 ⟨**3**⟩0 ⟨**6**⟩1 ⟨**0**⟩⟨**7**⟩ *decode* in Idx-form, e.g ⟨**7**⟩1 ⟨**3**⟩1 ⟨**9**⟩0 . . . ⟨**3**⟩1 ⟨**0**⟩⟨**4**⟩, to

⌞.....⌟.
As 20 bits, it is
⌞.....⌟
having used *Ziv* seeded with ⟨**0**⟩=‘’, ⟨**1**⟩=‘1’, and ⟨**2**⟩=‘0’.
Employing our fivebit-code, the 20 bits decode to symbols ⌞.....⌟ ⌞.....⌟ ⌞.....⌟ ⌞.....⌟.

Z7: Fri. 22 Mar Bits 01001010100100001110001101101100111 *decode* in Idx-form, e.g ⟨**7**⟩1 ⟨**3**⟩1 ⟨**9**⟩0 . . . ⟨**3**⟩1 ⟨**0**⟩⟨**4**⟩, to

⌞.....⌟.
As 15 bits, it is
⌞.....⌟
having used *Ziv* seeded with ⟨**0**⟩=‘’, ⟨**1**⟩=‘1’, and ⟨**2**⟩=‘0’.
Employing our fivebit-code, the 15 bits decode to symbols ⌞.....⌟ ⌞.....⌟ ⌞.....⌟.

Z8: Wed. 27 Mar ? Using dictionary 0: ε, 1: “1”, 2: “0”, compute EnZiv(11001010)= ⌞.....⌟, in ⟨**7**⟩1⟨**34**⟩0 . . . notation. In bits, EnZiv(11001010) is

⌞.....⌟.

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.) *Write **DNE** in a blank if the described object does not exist or if the indicated operation cannot be performed.*

Phi1: $N := \varphi(100) =$ ____. So $\varphi(N) =$ ____. EFT says that $3^{165} \equiv_N$ ____ $\in [0\,..\,N)$. Hence (by EFT) last two digits of $7^{[3^{165}]}$ are ____.

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

RS1: With $M := 22$ and $J := [0\,..\,M)$, use *repeated-squaring* to compute $6^{4096} \equiv_M$ ____ $\in J$. Since 4101 equals $2^{12} + 2^2 + 2^0$, the power $6^{4101} \equiv_M$ ____ $\in J$.
[*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 **J** be $(-290\,..\,290]$. There is a ring-iso $F: \mathbb{Z}_A \times \mathbb{Z}_B \to \mathbb{Z}_U$ sending (α, β) to $\langle G\alpha + H\beta \rangle_U$, using magic numbers $G =$ ____ $\in$**J** and $H =$ ____ $\in$**J**. A mod-U root of poly $h(x) := 20 \cdot [x+9]^3 + 29 \cdot [x-4]$ is $($____, ____$) \overset{F}{\mapsto$ ____ $\in$**J**.

CRT2: i Show all steps, except the ↯ tables, to compute a magic tuple **G** so that $g: \mathbb{Z}_5 \times \mathbb{Z}_6 \times \mathbb{Z}_7 \to \mathbb{Z}_{210}$ 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 $\boxed{h(x) \equiv_{210} 0}$, displaying the results in a table which shows *which* 3tup each came from. There are (not counting multiplicities) $K :=$ ____ 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) $\overset{\text{All}}{\ldots}$ (Cj). Then $z_2 =$ ____; $z_3 =$ ____.

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) $\overset{\text{All}}{\ldots}$ (Cj). Then $z_2 =$ ____; $z_3 =$ ____; $z_4 =$ ____.

CRT5: Let $f(x) := x^2 - 9x + 14$, and $N := 30425 \overset{\text{note}}{=\!=} p \cdot 25$, where $p := 1217$ is prime. The *number* of solns $x \in [0\,..\,N)$ to $\boxed{f(x) \equiv_N 0}$ is $K =$ ____. A number $Z \in [0\,..\,N)$ such that $f(Z) \neq 0$ yet $f(Z) \equiv_N 0$ is ____.
[*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. . . .
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^{th} Gregorian month. So $G(2) = 8$, since the 2^{nd} month is "February". The only fixed-point of G is ____. The *set* of posints k where $G^{\circ k}(12) = G^{\circ k}(7)$ is ____.
[January, February, March, April, May, June, July, August, September, October, November, December]

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

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

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* $H =$ ____.

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 ____.
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:$\frac{12}{66}$ $\mathcal{M}$:$\frac{5}{66}$ O:$\frac{7}{66}$ $\mathcal{R}$:$\frac{4}{66}$ $\mathcal{S}$:$\frac{32}{66}$ $\mathcal{T}$:$\frac{6}{66}$

codes these to bitstrings: I: ⌞ . . . . . ⌟ $\mathcal{M}$: ⌞ . . . . . ⌟

O: ⌞ . . . . . ⌟ $\mathcal{R}$: ⌞ . . . . . ⌟ $\mathcal{S}$: ⌞ . . . . . ⌟ $\mathcal{T}$: ⌞ . . . . . ⌟.

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 "000100010111111111011010 01", via the Elias code, decodes to ⌞ . . . . . ⌟, a sequence of *natnums* [hint: gun-blip-blip], followed by noise-bits ⌞ . . . . . ⌟.

Conv, Elias(84)= ⌞ . . . . . ⌟ (bitstring)

cZ1 Using dictionary 0: ε, 1: "1", 2: "0", compute EnZiv(11001010)= ⌞ . . . . . ⌟, in ⟨**7**⟩1⟨**34**⟩0... notation. In bits, EnZiv(11001010) is ⌞ . . . . . ⌟.

cZ2 Bits 010010101001000011100011011011001 11 *decode* in Idx-form, e.g ⟨**7**⟩1 ⟨**3**⟩1 ⟨**9**⟩0 . . . ⟨**3**⟩1 ⟨**0**⟩⟨**4**⟩, to ⌞ . . . . . ⌟.

As 15 bits, it is ⌞ . . . . . ⌟ having used *Ziv* seeded with ⟨**0**⟩='', ⟨**1**⟩='1', and ⟨**2**⟩='0'.

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

Playing with fields

C1 Blanks∈ℝ. So $\frac{1}{2+3i}$= ⌞ . . . . . ⌟ $+i\cdot$[⌞ . . . . . ⌟].

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

By the way, $|5-3i|$ = ⌞ . . . . . ⌟.

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

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