NT Summer
MAS4203 4801

Class-B

Prof. JLF King
Monday, 25Jul2016

Please *fill-in* every *blank* on this sheet. [50 minute exam, *or so Prof. Erroneous thought.*]

B1: *Show no work.*

a Prof. King believes that writing in complete, coherent sentences is crucial in communicating Mathematics, improves posture, and whitens teeth. Circle one:

True! **Yes!** ***wH'at S a?sEnTENcE***

b Define the ***numeral map*** $h{:}[1\,..\,12]\circlearrowright$, where $h(n)$ is the number of letters in the n^{th} numeral. So $h(12)$ equals 6, since "twelve" has 6 letters.

Compute the convolution $[h \circledast \boldsymbol{\mu}](10) =$ ____.

Convolve the night away... Our $[h \circledast \boldsymbol{\mu}](10)$ equals

$$h(1)\boldsymbol{\mu}(10) + h(2)\boldsymbol{\mu}(5) + h(5)\boldsymbol{\mu}(2) + h(10)\boldsymbol{\mu}(1)$$
$$= 3{\cdot}1 + 3{\cdot}[\text{-}1] + 4{\cdot}[\text{-}1] + 3{\cdot}1 = \text{-}1\,.$$

c 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

$z_2 =$ 33 ; $z_3 =$ 249 ; $z_4 =$ 753 .

Nuclear Fusion: I regret that I did not arrange the third fusion to be *DNE*. Fusing of (C1) with (C2) yields $C_{1,2}: z \equiv_{72} 33$. Continuing,

```
-----------------------------------------------------------
With A:=72 and B:=21, is there an x with
 x =A= 33 and | YES;  D := Gcd(A,B) = 3  divides 33-18 =: F.
 x =B= 18 ?   | Their ratio is  R := F/D = 5.
 -------------'
LBolt gives -2A + 7B =  D.  Multiplying by R produces
            -10A - -35B =  F  =  33 - 18.

Thus  x + -10A  =  33.  So  x := 753  solves both
congruences.  Reducing mod  L := Lcm(A,B)=504 gives

                x := [753  mod  L]  =  249.

Upshot:  Fuse((72, 33), (21, 18))  =  (504, 249).

-----------------------------------------------------------
With A:=504 and B:=10, is there an x with
x =A= 249 and | YES;  D := Gcd(A,B) = 2  divides  249-3 =: F.
x =B=   3 ?   | Their ratio is  R := F/D = 123.
--------------'
LBolt gives -2A + 101B =  D.  Multiplying by R produces
          -246A - -12423B =  F  =  249 - 3.

Thus  x + -246A  =  249.  So  x := 124233  solves both
congruences.  Reducing mod  L := Lcm(A,B)=2520 gives

               x := [124233  mod  L]  =  753.

Upshot:  Fuse((504, 249), (10, 3)) = (2520, 753).
```

d Let $N := 5^8$. Then $x^2 + y^2 = N$, where posints $x < y$ and $x \perp y$. [*Hint:* Use "repeated SOTS-melding". Only three melds needed.]

$x =$ 336 and $y =$ 527 .

Meld: Let $\mathcal{M}()$ be: Meld() followed by applying abs-value, then putting the smaller elt on the left of the pair. Construct m_j, a cop-SOTS pair for 5^{2^j}. Note $m_0 := (1,2)$ is a SOTS for $5^1 = 5^{2^0}$. So

$$m_1 := \mathcal{M}(m_0, m_0) = (3,4)\,;$$
$$m_2 := \mathcal{M}(m_1, m_1) = (7,24)\,;$$
$$m_3 := \mathcal{M}(m_2, m_2) = (336,527)\,.$$

e TMWFIt, 8 is a mod-125 primroot, since its mult-order (mod 125) is 100 $\overset{\text{note}}{=\!=} \varphi(125)$. Use the CRT-isomorphism to compute the corresponding mod-250 primroot $R =$ ____ $\in [0\,..\,250)$.

Primroot plan: Ring-iso $g{:}\,\mathbb{Z}_2 \times \mathbb{Z}_{125} \hookrightarrow \mathbb{Z}_{250}$, engenders group-iso $g{:}\,\Phi_2 \times \Phi_{125} \hookrightarrow \Phi_{250}$, whence $R = g\big((1,8)\big)$.

With moduli $M_1 := 2$ and $M_2 := 125$, guess/LBolt gives $1{\cdot}M_2 + [\text{-}62]{\cdot}M_1 = 1$, giving magic $G_1 := 1{\cdot}M_2 = 125$ and $G_2 := [\text{-}62]{\cdot}M_1 = \text{-}124$. Thus $g\big((1,8)\big)$ equals

$$1{\cdot}G_1 + 8{\cdot}G_2 = \text{-}867 \equiv_{250} 133\,.$$

[*Check:* $133 \equiv_2 1$ and $133 \equiv_{125} 8$, i.e $g^{-1}(133) = (1,8)$.]

f $S(98,000,000) =$ ____ where, for posints k, let $S(k)$ be the number of mod-k square-roots of 1. BTWay, group $\big(\Phi(1024), \cdot, 1\big)$ is isomorphic to this product ____ of cyclic groups.

[Let $\mathbf{C}(N)$ denote the cyclic group with N many elements.]

Sqroots of 1. Factoring, $N := 98,000,000 = 2^7 \cdot 5^6 \cdot 7^2$. By our Primroot thm, groups $\Phi(5^6)$ and $\Phi(7^2)$ are cyclic [and of even order], hence each has 2 sqroots, yielding $2{\cdot}2 = 4$ sqroots in their cartesian-product.

Group $\Phi(2^7)$ is isomorphic to a product of cyclic groups, $\mathbf{C}(2) \times \mathbf{C}(2^5)$. So it has $2{\cdot}2 = 4$ sqroots, as well. Hence our Φ_N has $2^4 = 16$ sqroots of 1. [So $|\mathbb{QR}_N| = \varphi(N)/16$.]

Finally, $\Phi(1024) \cong \mathbf{C}(2^1) \times \mathbf{C}(2^8) = \mathbf{C}(2) \times \mathbf{C}(256)$.

OYOP: *In grammatical English* ***sentences****, write your essays on every* ***third*** *line* (usually)*, so that I can easily write between the lines. Do* **not** *restate the question. Start each essay on a* ***new*** *sheet of paper.*

B2: Note $f(n) := \frac{1}{2}\cdot[27^n + 31^n]$ is an integer. Prove, for each *odd* $n \geqslant 5$, that $f(n)$ is composite. [*Hint:* Look at $f(n)$ mod something.]

Composite: If a modulus divides $f(\text{Odd})$, then it likely divides $f(1) \overset{\text{note}}{=\!=} 29$ too. With $S_n := [27^n + 31^n]$, observe $\boxed{S_{\text{Odd}} \equiv_{29} [-2]^{\text{Odd}} + 2^{\text{Odd}} = 0}$. Since 27 and 31 have the same parity, our S_n is always even. Hence each $f(n) \in \mathbb{Z}$ and $f(\text{Odd}) \bullet\!\!-\!\!| 29$.

Our f is strictly increasing, so $f(d) > f(1) = 29$ for each $d>1$. Hence 29 is a **proper** divisor of $f(\text{Odd}>1)$.

B3: For prime p, the units group $\Gamma := \Phi_p$ is cyclic of order $p-1$. Let $\mathcal{S}$ be its set of generators [those elts of order $p-1$]. For $p>3$, prove $\prod(\mathcal{S}) \equiv_p 1$. [Use Wilson's-Thm ideas.]

Get involved! If $\langle 1/x\rangle = x$, i.e $x^2=1$, then $\text{Ord}_\Gamma(x) \leqslant 2$. So $\text{Ord}_\Gamma(x) < p-1$, hence x is **not** a Γ-generator.

Suppose we knew that $[x \in \mathcal{S} \overset{*}{\Longrightarrow} \langle 1/x\rangle \in \mathcal{S}]$. Then involution $h{:}\mathcal{S}\circlearrowleft$ is well-defined. Hence

$$\prod(\mathcal{S}) \;=\; \prod\big(\text{Fix}(h)\big) \;=\; \prod(\varnothing) \;=\; 1\,, \quad \text{as desired.}$$

To establish $(*)$, let $\mathbf{X}, \mathbf{Y}$ be the orders of Γ-elements x, y, where $x{\cdot}y = 1$. Thus $y^{\mathbf{X}} = x^{\mathbf{X}}y^{\mathbf{X}} = [xy]^{\mathbf{X}} = 1$. So $\mathbf{X} \bullet\!\!-\!\!| \mathbf{Y}$. Similarly, $\mathbf{Y} \bullet\!\!-\!\!| \mathbf{X}$. But both $\mathbf{X},\mathbf{Y} > 0$, so $\mathbf{X} = \mathbf{Y}$.

B1:	___ ___ ___	120pts
B2:	___ ___	45pts
B3:	___ ___	40pts
Total:	___ ___ ___	205pts