Number Theory
MAT4930 *4D70*

Quizzes Q

Summer 2018

Number Sets. An expression such as $k \in \mathbb{N}$ (read as "k is an element of $\mathbb{N}$" or "k in $\mathbb{N}$") means that k is a natural number; a ***natnum***.

$\mathbb{N}$ = 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 ***ratnums*** and $\mathbb{Q}_-$ for the negative ratnums.

$\mathbb{R}$ = reals. The ***posreals*** $\mathbb{R}_+$ and the ***negreals*** $\mathbb{R}_-$.

$\mathbb{C}$ = complex numbers, also called the ***complexes***.

An "***interval of integers***" $[b\,..\,c)$ means the intersection $[b, c) \cap \mathbb{Z}$; ditto for open and closed intervals. So $[\mathsf{e}\,..\,2\boldsymbol{\pi}] = \{3, 4, 5, 6\} = [3\,..\,6] = (2\,..\,6]$. We allow b and c to be $\pm\infty$; so $(-\infty\,..\,\text{-}1]$ is $\mathbb{Z}_-$.

Floor function: $\lfloor \boldsymbol{\pi} \rfloor = 3$, $\lfloor \text{-}\boldsymbol{\pi} \rfloor = \text{-}4$. Ceiling fnc: $\lceil \boldsymbol{\pi} \rceil = 4$. Absolute value: $|\text{-}6| = 6 = |6|$ and $|\text{-}5 + 2\boldsymbol{i}| = \sqrt{29}$.

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*'. CoI: '*Constant of Integration*'. LoI: '*Limit(s) of Integration*'.

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 Sqroot: '*square-root*', e.g, "the sqroot of 16 is 4". Ptn: '*partition*', <u>*but*</u> 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 $\log(x) := \int_1^x \frac{\mathrm{d}v}{v}$. Its inverse-fnc is $\exp()$. For $x>0$, then, $\exp(\log(x)) = x = \mathsf{e}^{\log(x)}$. For real t, naturally, $\log(\exp(t)) = t = \log(\mathsf{e}^t)$. PolyExp: '*Polynomial-times-exponential*'. E.g, $F(t) := [3 + t^2] \cdot \mathsf{e}^{4t}$ is a polyExp.

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".

Q1: Thu. 05 Jul LBolt gives $G := \text{GCD}(413, 294) =$ ______ . And $413S + 294T = G$, where $S =$ ______ & $T =$ ______ are integers.

Also $x =$ ______ $\in [0\,..\,13)$ solves congr. $5x \equiv_{13} 3$.

Q2: Fri. 06 Jul LBolt: GCD(70, 42)= ________ ·70 + ________ ·42.

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

Q3: Mon. 09 Jul Mod K:=50, the recipr. $\langle \frac{1}{21} \rangle_K =$ ________ $\in [0 .. K)$.

The last two digits of 29^{128} are ____ ____. [Hint: Use repeated-squaring, and look for a pattern.]

Q4: Tue. 10 Jul Euler $\varphi(36300) = 2^A \cdot 3^B \cdot 5^C \cdot 7^D \cdot 11^E$, where $A=$ ________, $B=$ ________, $C=$ ________, $D=$ ________, $E=$ ________.

As a single number, $\tau(36300) =$ ________.

Q5: Wed. 11 Jul

With M:=88, congruence $36x \equiv_M 28$ has $N=$ ________ solns in $[0 .. M)$. The *smallest* such is $S=$ ________.

As $k = 0, 1, \ldots,$ ________, formula $S + [kB]$ gives *all* solns in $[0 .. M)$, where $B=$ ________.

Q6: Thu. 12 Jul With $M := 22$ and $\mathbf{J} := [0 .. M)$, use *repeated-squaring* to compute $6^{1024} \equiv_M$ ________ $\in \mathbf{J}$. Since 1033 equals $2^{10} + 2^3 + 2^0$, power $6^{1033} \equiv_M$ ________ $\in \mathbf{J}$.

[*Hint:* Compute with symm. residues, and use periodicity.]

Q7: Mon. 16 Jul *Magic integers* G_1, G_2, G_3, each in $[0..330)$, are such that the $g{:}\mathbb{Z}_5 \times \mathbb{Z}_6 \times \mathbb{Z}_{11} \to \mathbb{Z}_{330}$ 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 $G_3 =$ .... $\in [0..330)$. Also: "Element $g((6, 11, 5))$ is a zero-divisor in $\mathbb{Z}_{330}$." (Circle) *T* *F*

Q8: Mon. 06 Aug Since $221 = 13 \cdot 17$, then $221 = a^2 + b^2$ where $a \perp b$ and posints $a=$ .... $\leqslant b=$ ....

Doubling, $442 = x^2 + y^2$, where $x \perp y$ are posints, and $x =$ .... $\leqslant y =$ ....

Q9: Tue. 07 Aug

A primitive Pythagorean triple has $a^2 + 28^2 = c^2$, where $a =$ .... and $c =$ .... with $a \perp c$.

That's All, Folks!

Mr. Green's will left *half* of his estate to his eldest, Abe; a *quarter* to Bert; and an *eighth* to his youngest, Carl. Alas, his "estate" comprises 7 horses; and nobody wants a fractional horse. [It's messy for the humans… —and uncomfortable for the horse.]

What to do?

Ta da! Nancy NumberTheorist rides up and adds her horse to the 7, making 8. She gives 4 horses to Abe, 2 to Bert, 1 horse to Carl, then rides off on her own horse, well contented.

Whoa! Each child got more than his fair share of the estate, receiving his fraction out of 8 horses, rather than 7. And yet, Nancy lost nothing; she rides off into the Sunset, on Sunset [the name of her horse].

Explain this