NT-Cryptography
MAT4930 *7554*

Quizzes R

Spring 2016

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 = $\{0, 1, 2, \ldots\}$.

$\mathbb{Z}$ = integers = $\{\ldots, -2, -1, 0, 1, \ldots\}$. For the set $\{1, 2, 3, \ldots\}$ 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 $[e \,..\, 2\pi] = \{3, 4, 5, 6\} = [3 \,..\, 6] = (2 \,..\, 6]$. We allow b and c to be $\pm\infty$; so $(-\infty \,..\, -1]$ is $\mathbb{Z}_-$.

Mathematical objects. Seq: '*sequence*'. poly(s): '*polynomial(s)*'. irred: '*irreducible*'. Coeff: '*coefficient*' and var(s): '*variable(s)*' and parm(s): '*parameter(s)*'. Expr.: '*expression*'. CoI: '*Constant of Integration*'. LoI: '*Limit(s) of Integration*'.

Fnc: '*function*' (so ratfnc: means rational function, a ratio of polynomials). cty: '*continuity*'. cts: '*continuous*'. diff'able: '*differentiable*'.

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*', but pt: '*point*', as in "a fixed-pt of a map".

FTC: '*Fund. Thm of Calculus*'. IVT: '*intermediate-Value Thm*'. MVT: '*Mean-Value Thm*'. CoV: '*Change-of-Variable*'.

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*'. QED: *quod erat demonstrandum*, meaning "end of proof".

R1: Wed. 20 Jan LBolt gives $G := \text{Gcd}(413, 294)=$ ______ . And $413S + 294T = G$, where $S=$ ______ & $T=$ ______ are integers.

R2: Mon. 25 Jan Mod $K{:=}50$, the recipr. $\langle\frac{1}{21}\rangle_K =$ ______ $\in [0 \,..\, K)$. [*Hint:* ↯] So $x=$ ______ $\in [0 \,..\, K)$ solves $4 - 21x \equiv_K 1$.

R3: Wed. 27 Jan LBolt: $\text{Gcd}(51, 85)=$ ______ $\cdot 51$ + ______ $\cdot 85$.

So (LBolt again) $G := \text{Gcd}(51, 85, 15)=$ ______ and ______ $\cdot 51$ + ______ $\cdot 85$ + ______ $\cdot 15 = G$.

R4: Mon. 01 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 $[5 \cdot 11] \bullet\!| \; G_1$ and analogously for G_2 and G_3.

R5: Fri. 12 Feb **a** Suppose $y \in \mathrm{QR}_N$, where N is oddprime. You compute Bézout mults U and V st. $yU + NV = 1$. Then "*U is a mod-N square*" is: AT AF Nei

b With $p := 323$, and $H := \frac{p-1}{2}$, note $66^H \equiv_p -2$. Thus p is ______ .

R6: Mon. 15 Feb Integer $M := 23$ is prime. $\boxed{\text{Circle}}$ each of the M-QRs, below. [*Hint:* At least two can be done by inspection.]

$$-1 \qquad 6 \qquad 7 \qquad 19$$

R7: Fri. 26 Feb Since $4800 = 2^6 \cdot 3 \cdot 5^2$, it has ______ many positive divisors. [Write ANS naturally as a product of integers.]

R8: Mon. 07 Mar 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 $p_1 < p_2 < \ldots$.

For a prime q and natnum N, the divisor-sum is

$\sigma(q^N) =$ ______ $=$ ______.

R9: Fri. 11 Mar Three Jacobi symbols: Two blanks are immed.:

$\left(\frac{4203}{2006}\right) =$ ______. $\left(\frac{4203}{99}\right) =$ ______. $\left(\frac{120}{27113}\right) =$ ______.

Fix a prime q and natnums N and K. Then a closed-formula

for σ_N is: $\sigma_N(q^K) =$ ______.

RA: Mon. 18 Apr The 1948 paper that introduced information-theoretic entropy was written by $\boxed{\text{Circle}}$:

DNE **Archimedes** **Euler** **Fuchs** **Gauss**

Meshalkin **Shannon** **Sinai** **Ziv**