Staple!

Team X_____

Number Theory 2
MAT4930 5662

Home-X

Prof. JLF King
Touch: 2Jul2018

Hello. This Gentle Exam is due **4PM, Sunday, 12Nov2006**, slid under LIT402.

Essays. *Write in complete sentences and also fill-in the blanks. Each (typed!) essay starts a new page.* Essays violate the CHECKLIST at *Grade Peril*!

Use **B** for the time-unit needed by your computer to produce a random bit. So to uniformly pick an $n \in [0\,..\,2^k)$ takes time $k\mathbf{B}$.

Take a positive integer N between two powers of two: $2^{k-1} < N < 2^k$. We showed that a unif. choice can be made from $[0\,..\,N)$ in

$$\text{Expected-time} \leqslant k\mathbf{B} \cdot N/2^{k-1} \overset{\text{note}}{\leqslant} 2k\mathbf{B}\,.$$

The fantasy-land assumption: For convenience in some problems below: Imagine, regardless of the size of posint j, that we can unif.-pick an elt of $[0\,..\,j)$ in constant-time, call it **G**. □

X1: Solve exercise **7.14***P*166. First suppose that M is too large to be factored.

Now suppose that $M = p_1 \cdot \ldots \cdot p_L$ into distinct primes. What speed improvements can you make? (Does the Chinese Remainder Thm help?) What about the general factored case?

X2: Solve exercises **7.18,7.19***P*167. For **7.18**, please show that the expected number of **G** choices is $+\infty$.

For **7.19**, compute $\mathcal{E}_{\mathbf{G}}=$ ⌞. . . . . ⌟, the expected number of choices **G**. Now give a good upper-bound for $\mathcal{E}_{\mathbf{B}}=$ ⌞. . . . . ⌟, the expected number of bit-choices. Explain all your arguments carefully in your essay.

X3: Please solve **9.7***P*218.

X4: Consider a $\mathbb{Q}$-irreducible poly $h(z) = z^2 - Sz + P$; so $S, P \in \mathbb{Q}$. There are complex numbers $\boldsymbol{\alpha}, \boldsymbol{\beta}$ st.

$$h(z) \;=\; z^2 - Sz + P \;=\; [z - \boldsymbol{\alpha}] \cdot [z - \boldsymbol{\beta}]\,.$$

i Prove that $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$. Let $\mathbf{F} := \mathbb{Q}[\![\boldsymbol{\alpha}]\!] \overset{\text{note}}{=\!=} 1\cdot\mathbb{Q} + \boldsymbol{\alpha}\cdot\mathbb{Q}$. This is a $\mathbb{Q}$-vectorspace and field. Prove $\mathbb{Q}[\![\boldsymbol{\beta}]\!] = \mathbf{F}$.

On **F**, define an involution, ***h*-conjugation**:

$$\overline{1} := 1, \quad \overline{\boldsymbol{\alpha}} := \boldsymbol{\beta}, \quad \overline{\boldsymbol{\beta}} := \boldsymbol{\alpha}.$$
$$\overline{\zeta} := x - y\boldsymbol{\beta} \quad \text{where} \quad \zeta := x - y\boldsymbol{\alpha}\,.$$

First show that this map is *well-defined*. Now prove that $\zeta \mapsto \overline{\zeta}$ is a field-automorphism.

Define a ***norm*** $\mathcal{N}\!:\!\mathbb{Q}[\![\boldsymbol{\alpha}]\!] \to \mathbb{Q}$ by

J1: $$\mathcal{N}(\zeta) \;:=\; \mathcal{N}_h(\zeta) \;:=\; \zeta \cdot \overline{\zeta} \overset{\text{note}}{=\!=} x^2 - xyS + y^2P\,.$$

Prove $\forall\, \zeta, z \in \mathbf{F}$: $\mathcal{N}(\zeta \cdot z) = \mathcal{N}(\zeta) \cdot \mathcal{N}(z)$ and $\boxed{\mathcal{N}(\zeta) = 0 \;\; \text{IFF} \;\; \zeta = 0}$.

ii Now assume $S, P \in \mathbb{Z}$. Let $\Gamma := \mathbb{Z}[\![\boldsymbol{\alpha}]\!]$; show $\mathbb{Z}[\![\boldsymbol{\beta}]\!] = \Gamma$. Prove $\mathcal{N}$ maps Γ into $\mathbb{Z}$. Prove $\forall \zeta \in \Gamma$:

J2: $$\mathcal{N}(\zeta) \in \mathbb{U}_{\mathbb{Z}} \;\; \text{IFF} \;\; \zeta \in \mathbb{U}_\Gamma\,.$$

Here $\mathbb{U}_\Gamma$ is the set of Γ-units.

iii Let $\boldsymbol{\alpha} := \sqrt{5}$. Prove that $\Lambda := \mathbb{Z}[\![\boldsymbol{\alpha}]\!]$ is *not* a UFD, by noting that

$$-2 \cdot 2 \;=\; -4 \;=\; [1 - \boldsymbol{\alpha}] \cdot [1 + \boldsymbol{\alpha}]\,.$$

Prove that elts ± 2 and $1 \pm \boldsymbol{\alpha}$ are each Λ-irred, and that none is Λ-prime. [*Hint:* For irreducibility: You can use the multiplicativity of the norm, and (J2), working modulo something.]

End of Home-X

X1:	___ ___ ___	110pts
X2:	___ ___ ___	110pts
X3:	___ ___	35pts
X4:	___ ___ ___	110pts
Total:	___ ___ ___	365pts

HONOR CODE: *"I have neither requested nor received help on this exam other than from my team-mates and my professor (or his colleague)."* *Name/Signature/Ord*

Ord: ⌞. . . . . ⌟⌞.⌟⌞.⌟

Ord: ⌞. . . . . ⌟⌞.⌟⌞.⌟

Ord: ⌞. . . . . ⌟⌞.⌟⌞.⌟