Staple!

Name: ______________________ **Ord:** ___ ___

NT-Cryptography MAT4930 *0329* | **IndividualOP-X** | Prof. JLF King Fri, 21Apr2023

Cryp IOP is due **2PM, Thurs., 27Apr2023**, slid *completely* under my office door, 402 LITTLE HALL. This sheet is "Page $1/N$", and you've labeled the rest as "Page $2/N$"…"Page N/N".

Essays must be TYPED, *and* (preferably) *double-spaced. Use the* Print/Revise ↻ *cycle to produce good, well thought out, essays. Do* **not** *restate the problem; just solve it.*

X1: In ring $\Gamma := \mathbb{Z}_7[x]$, consider polynomials

$$r_0 := x^4 - 2x^3 + x - 2\,,$$
$$r_1 := x^3 + 3x^2 - 3x\,.$$

Using symmetric residues: Compute (and exhibit) an LBolt table which computes polys $\mathcal{G} := \text{GCD}(r_0, r_1)$ and $S.T$ s.t $\mathcal{G} = Sr_0 + Tr_1$. [The table is tiny; can be computed by hand.]

Extra credit: Write your own program (showing the code, and two sample runs over different primes) which computes and prints LBolt tables over $\mathbb{Z}_p[x]$, where p is prime.

X2: For alphabet size $\Gamma \in [2\,..\,\infty)$, consider a *finite*, complete (Kraft-sum equals 1) UD-code $\mathcal{C}$. Prove that $R \equiv_{\Gamma-1} 1$, where R is the number of codewords.

X3: The building block of a cryptosystem uses N-*Serial* numbers, for large values of N. (Defns are below.)

i Prove: *For each positive integer N, there exists an N-Serial number.*

ii Produce (with proof, 'natch) a 5-Serial number $V=$ ______________ . (A little extra credit: Can you prove or computer-search that your V is the *smallest* 5-Serial number?)

Defns. An posint $\mathbf{S}$ is ***Cubish*** if it is divisible by some member of $\{8, 27, 64, 125, 216, \ldots, k^3, \ldots\}$; otherwise $\mathbf{S}$ is ***Flat***. (E.g $0, 162, 375$ are Cubish, and $1, 12, 90, 36$ are Flat.)

For N,$\mathbf{S}$ posints, our $\mathbf{S}$ is "***N-Serial***" if *each* member of $\{\mathbf{S}+j\}_{j=0}^{N-1}$ is Cubish. [E.g, $\mathbf{S}=80$ is 2-Serial, since $8 \mid 80$ and $27 \mid 81$, but 80 is not 3-Serial, as no cube divides 82. Another example: 375 is 2-Serial but not 3-Serial.]

X4: Prime $q \equiv_4 1$ is such that $p := 1 + 2q$ is prime. Prove that 2 is a p-primroot. [E.g, $(q, p) = (5, 11), (29, 59), (41, 83), (53, 107), (89, 179), (113, 227), \ldots$.]

[*Hint:* The number of p-primroots is $\varphi(\varphi(p))$. State and prove lemmas about the possible mult-orders of NQRs and QRs mod-p.]

HONOR CODE: *"I have neither requested nor received help on this exam other than from my professor."*

Signature: ______________________________________

Folks, I've had a great time learning NT & Codes with you. It's been a pleasure having a lively (and funny) *class of Enthusiastic NTers. Stop by in future semesters for Math/chess/frisbee/pickleball…*

Cheers, Prof. K