

X1: Show no work. Please write DNE in a blank if the described object does not exist or if the indicated operation cannot be performed.

a $S(98,000,000) = \dots$ where, for posints k , let $S(k)$ be the number of mod- k square-roots of 1. BTWay, group $(\Phi(1024), \cdot, 1)$ is isomorphic to this product \dots of cyclic groups. [Let $C(N)$ denote the cyclic group with N many elements.]

b $N := \varphi(100) = \dots$. So $\varphi(N) = \dots$. EFT says that $3^{1621} \equiv_N \dots \in [0..N)$. Hence (by EFT) last two digits of $7^{[3^{1621}]}$ are \dots .

c Modulo 309, the multiplicative-order of 5 is \dots . [Hint: $\varphi(309)$ has very few prime factors.]

d Three Jacobi symbols: Two blanks are immed.: $\left(\frac{51}{289}\right) = \dots$, $\left(\frac{-353}{902491}\right) = \dots$, $\left(\frac{7554}{4930}\right) = \dots$

OYOP: Your 2 essay(s) must be TYPESET, and Double or Triple spaced. Use the Print/Revise \odot cycle to produce good, well thought out, essays. Start each essay on a NEW sheet of paper.

Do not restate the problem; just solve it.

X2: As polynomials in $\Gamma := \mathbb{Z}_7[x]$, let

$$B(x) := x^4 - 2x^3 + x - 2;$$

$$C(x) := x^3 + 3x^2 - 3x.$$

Write t.fol polys, using coeffs in $[-3..3]$; use \equiv for equality in \mathbb{Z}_7 and in Γ . Compute quotient and remainder polys, $q(x) \equiv \dots$ & $r(x) \equiv \dots$, with $B \equiv [q \cdot C] + r$ and $\text{Deg}(r) < \text{Deg}(C)$. Let $D := \text{Gcd}(B, C)$. **Monic** $D(x) \equiv \dots$

Compute polys $S(x) \equiv \dots$, $T(x) \equiv \dots$ st. $[S \cdot B] + [T \cdot C] \equiv D$.

X3: **i** Use Pollard- ρ to find a non-trivial factor of $M := 59749$, using seed $s_0 := 7$ and map $f(x) := 1+x^2$. Make a nice table, labeled

$$\text{Time} \mid \text{Tortoise} \mid \text{Hare} \mid s_{2k} - s_k \mid \text{Gcd}(??)$$

—but **replace** the “??” with the correct expression. You found non-trivial factor $E := \dots$

The hare Hits into the tortoise at time $H := \dots$

Repeat, showing the table for $s_0 := 24$. Experiment with different seeds; what is the typical running time? How is it related to the factor you find?

ii A seed s determines a **tail**; the smallest natnum T for which there is a time $n > T$ with $f^n(s) = f^T(s)$. The smallest such n is $T+L$ where L is the **period**. Derive (picture+reasoning) a formula for the hitting time $H(T, L)$. [Hint: $H(0, L) = L$.]

iii Produce a Floyd-done-twice algorithm that computes both T and L . The number, N , of f -evaluations is upper-bounded by some small constant times $T+L$ (=arclength of ρ). How small can you get $N(T, L)$? [Hint: $N(0, L) = 3L$.]

End of Home-X

X1: _____ 110pts

X2: _____ 90pts

Poorly stapled, **X3:** _____ 125pts
or missing names or Honor code: _____ -15pts

Not typed/double-spaced: _____ -15pts

Total: _____ 325pts

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: _____