CS681 - COMPUTATIONAL NUMBER THEORY & ALGEBRA

NITIN SAXENA

ASSIGNMENT 1

POINTS: 50

DATE GIVEN: 11-JAN-2025 DUE: 31-JAN-2025

Rules:

- You are strongly encouraged to work *independently*. That is the best way to understand the subject.
- Write the solutions on your own and honorably *acknowledge* the sources if any. `cse.iitk.ac.in/pages/AntiCheatingPolicy.html`
- Clearly express the fundamental *idea* of your proof/ algorithm before going into the other proof details. The distribution of partial marks is according to the proof steps.
- There will be a penalty if you write unnecessary or unrelated details in your solution. Also, do not repeat the proofs done in the class.
- Submit your solutions, before time, to your TA. Preferably, submit a printed/pdf copy of your LaTeXed or Word processed solution sheet.

  Your TA will help in grading and doubt resolution: `Tufan Singha Mahapatra <tufansm@cse.iitk.ac.in>`
- Problems marked '0 points' are for practice.

Question 1: *[3+3 points]* Recall the definition of a ring and its *characteristic*. Which integers can be the characteristic of a ring? Of a *field*?

Question 2: (Finite field) *[4+5+6 points]* Let p be a prime number. Show that $k := (\mathbb{Z}/p\mathbb{Z}, +, \times)$ is a field.

- Can you construct a field of size p^2?
- What are the other finite fields, or finite *extensions* of k? What is the *union* of all of them?

For Qns. 3-4, let k be a finite field of characteristic p.

Question 3: (Cyclicity) *[5+3 points]* Show that the multiplicative group $k^* := k \setminus \{0\}$ is cyclic.

- Can you estimate the number of its *generators* (as a function of $|k|$)?

Question 4: (Repeated squaring) *[5 points]* Given $n \in \mathbb{N}$ and $x \in k$, we want to compute x^n. Estimate the best *time complexity* in bit operations.

Question 5: (Cyclotomy) *[11+5 points]* Let $n \in \mathbb{N}$. Show that the polynomial $(X^n - 1)$, over $\mathbb{Q}$, factorizes as:

$$X^n - 1 \;=\; \prod_{d|n} \varphi_d(X) \;,$$

where $\varphi_d(X)$ is an *irreducible* integral polynomial – called the *d-th cyclotomic polynomial*.

- Let R be a ring. Show that, in $R[X]/(\varphi_n(X))$:

$$\sum_{i=0}^{n-1} X^{ij} = 0 \;,$$

for every $j \in \mathbb{N}$ that is not a multiple of n. (Otherwise, the sum is n.)

Question 6: *[0 points]* Given n in binary and r in unary ($n, r \in \mathbb{N}$), we want to compute the polynomial $(X+1)^n$ modulo $\langle n, X^r - 1\rangle$. Estimate the best *time complexity* in bit operations.

Question 7: ($\sqrt[n]{1}$) *[0 points]* How many n-th *primitive* roots of unity are there in $\mathbb{C}$?

- in $\mathbb{F}_p$?

Question 8: (Local ring) *[0 points]* Let $\mathbb{F}$ be a field and $n \geq 0$. Show that the ring $\mathbb{F}[x]/\langle x^n\rangle$ cannot be *decomposed* into a product of two nonzero rings.

Question 9: (Prime ideal) *[0 points]* Consider the polynomial ring $R = \mathbb{F}[x_1, \ldots, x_n]$ and an ideal I of it. What should be the properties of I so that R/I is a domain? A field?

Question 10: *[0 points]* Show that any ideal I of the polynomial ring R is *finitely* generated, i.e. $\exists g_1, \ldots, g_m \in I$ s.t. $I = \langle g_1, \ldots, g_m\rangle_R$.

Question 11: *[0 points]* We saw that $\gcd(a, b)$, for $a > b > 1$, computation is a sequence of $O(\log b)$ divisions. Show that this bound is *tight* for some (input) numbers a, b.

Question 12: *[0 points]* We saw that $\gcd(a, b)$, for $a > b > 1$, computation is a sequence of divisions; where division by (say) b yields a remainder in $(-b/2, b/2]$. What happens to the time-complexity if we instead store the remainder as a nonnegative in $[0, b-1]$?

Question 13: (CRT) *[0 points]* Why does Chinese remaindering theorem on integers require *coprime* integers? Can it be generalized?

Question 14: (Convergence) *[0 points]* List the conditions under which Newton's approximation algorithm converges to a root x_i of a polynomial $f(x)$.

Give examples where it fails to converge.

□□□