CS 203B: Mathematics for Computer Science-III
Assignment 4

Deadline: 18 : 00 hours, September 4, 2015

General Instructions:

- Write your solutions by furnishing all relevant details (you may assume the results already covered in the class).
- You are strongly encouraged to solve the problems by yourself.
- You may discuss but write the solutions on your own. Any copying will get zero in the whole assignment.
- If you need any clarification, please contact any one of the TAs.
- Please submit the assignment at KD-213/RM-504 before the deadline. Delay in submission will cause deduction in marks.

Rings have found a number of applications in Computer Science. This includes designing cryptosystems and related problems, algorithms for machine learning, image recognition, error-correcting codes etc. In this assignment, we take a look at one of them: *primality testing*. In this problem, a number n is given and one needs to decide if it is prime. It can be done simply by trying to divide n by all numbers $\leq \sqrt{n}$, however, for large values of n (imagine 100 digit long numbers), this method takes too much time. Several faster methods to solve this problem are known. We describe one of them. It is an example of how the rings come to unexpected help in designing algorithms.

Question 1: [5]

Given number n, define ring $R = Z_n[x]/(x^r - 1)$ for a carefully chosen number r (r is much smaller than n; of the order of square of the number of digits in n). Prove that R is a finite ring with exactly n^r elements.

Question 2: [5]

An element of R is a polynomial in x of degree $< r$ with coefficients from Z_n. We use the notation $a(x)$ to represent elements of R. Define map $\phi : R \mapsto R$ as: $\phi(a(x)) = a^n(x)$. It is obvious that

$$\phi(a(x) \cdot b(x)) = \phi(a(x)) \cdot \phi(b(x)).$$

Prove that ϕ is a ring homomorphism if and only if

$$\phi(a(x)) = a(x^n)$$

for every $a(x) \in R$.

Question 3: [10] Prove that when n is prime, ϕ is a ring homomorphism.

Question 4: [5]

On the other hand, when n is a composite number, ϕ is not a ring homomorphism. Show this for the ring $Z_6[x](x^2 - 1)$. In fact, it can be shown that when n composite, the number of elements $a(x)$ of R for which $\phi(a(x)) = a(x^n)$ is less than $\binom{2r}{r}$.

Question 5: [10]

This difference in the properties of ϕ is exploited to decide if n is prime. Consider elements $x + \ell$ for $1 \leq \ell \leq r$. It can be shown that each of these elements is a unit of R. Let

$$S = \{\prod_{\ell=1}^{r} (x + \ell)^{m_\ell} \mid m_\ell \geq 0\}.$$

The operations in the above definition are of ring R. Set S is clearly a group under multiplication. Prove that the size of S is at least $\binom{2r}{r}$.

Question 6: [5] Once we have all the above properties, the algorithm is quite simple:

For every ℓ, $1 \leq \ell \leq r$, check if $\phi(x + \ell) = x^n + \ell$ in the ring R.

Prove that when n is composite, the above check will fail for at least one ℓ.