CS345: Assignment 10

Q1. Let $a, n \in \mathbb{Z}_m$. Let $gcd(n, m) = 1$ and $k = n^{-1}$ in $\mathbb{Z}_m$. Let $b = a.n)$. Show that $k.b = a(mod\ m)$.

Q2. Prove that $\mathbb{Z}_N$ is a commutative ring with unity, for any natural number N.

Q3. Find $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}(mod\ 7)$ using Fermat's little theorem.

Q4. Suppose that p and q are distinct primes, $a^p \equiv a(mod\ q)$, and $a^q \equiv a(mod\ p)$. Prove that $a^{pq} \equiv a \mod pq$.

Q5. Compute $1019^{-1}(mod\ 2058)$.

Q6. Describe an efficient procedure to compute $a^b(mod 10^9+7)$ where a and b may have hundreds of digits.

Q7. (i) Show that if N is an odd number, then the number of numbers which are coprime with N is even.

(ii) Using Fermat's little theorem and part(i) show that for any odd N, there exists a number R which is a power of 2 and $R^2 = 1(mod\ N)$.

Q8. Given an odd number N, let R be a power of 2 greater than N. Since N and R are coprime, $R^{-1} \in \mathbb{Z}_N$ and $N^{-1} \in \mathbb{Z}_R$. Let $x \in \mathbb{Z}_N$. Define a bijection $f : \mathbb{Z}_N \to \mathbb{Z}_N$, given by $f(x) = xR^{-1}(mod\ N)$. Consider Algorithm **??** to compute $fx)$.

Input: $x \in \mathbb{Z}_N$
$m := -x.N^{-1}(mod\ R)$;
$u := (x + m.N)/R$;
if $u \geq N$ **then**
| $u := u - N$;
end
return y;

Algorithm 1: $f(x) = xR^{-1}(mod\ N)$

(i) Prove that R divides $x + m.N$ to show that u is well defined.

(ii) Prove the correctness of the algorithm.

Observe that this algorithm does not require any division.

(iii) Design multiplication of two numbers in $\mathbb{Z}_N$ using function f such that it does not require any division operation. Hint: $y \equiv_N R^{-1}.R.y$.

(iv) Simplify the algorithm assuming that R is so chosen that $R^2 \equiv_N 1$.

Q9. Determine S-function and P-function for RSA Cryptosystem for prime numbers 17 and 37.

Q10. Prove that the polynomial obtained from interpolating on n distinct values, is unique.