Indian Institute of Technology Kharagpur

CS60094: Computational Number Theory, Spring 2023
Mid-Semester Examination

22 February 2023 | CSE 107, 2PM - 4PM | Total marks = 60

Answer *exactly five* questions. Keep your answers clear and concise. State all assumptions you make.

1. Suppose that $\gcd(r_0, r_1)$ is computed by the repeated Euclidean division algorithm. Assume $r_0 > r_1 > 0$. Let r_{i+1} denote the remainder obtained by the i-th division (that is, in the i-th iteration of the Euclidean loop). So the computation proceeds as $\gcd(r_0, r_1) = \gcd(r_1, r_2) = \gcd(r_2, r_3) = \cdots$ with $r_0 > r_1 > r_2 > \cdots > r_k > r_{k+1} = 0$ for some $k \geq 1$.

   If the computation of $\gcd(r_0, r_1)$ requires exactly k Euclidean divisions, show that $r_0 \geq F_{k+1}$ and $r_1 \geq F_k$. Here, F_n is the n-th Fibonacci number: $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. [12]

2. Let $m \in \mathbb{N}$ and $a_1, a_2, \ldots, a_t \in \mathbb{Z}_m^*$. Suppose that we want to compute $a_1^{-1}, a_2^{-1}, \ldots, a_t^{-1}$. Describe an algorithm to compute these modular inverses with just one call to the extended Euclidean algorithm and using at most $3t$ modular multiplications (modulo m). [12]

3. Solve the following system of congruences:

$$
\begin{aligned}
x &\equiv 17 \pmod{36} \\
x &\equiv 28 \pmod{40} \\
x &\equiv 3 \pmod{15}
\end{aligned}
$$

[12]

4. In the class, we have seen how to lift solutions to congruences of the form $f(x) \equiv 0 \pmod{p^e}$ to the solutions of $f(x) \equiv 0 \pmod{p^{e+1}}$. You will now modify the method slightly to lift roots of $f(x)$ modulo p^e to roots modulo p^{2e}.

   (a) Let $f(x)$ be a polynomial with integer coefficients, $e \in \mathbb{N}$ and z a solution of $f(x) \equiv 0 \pmod{p^e}$. Write $z' = z + kp^e$. Show how we can compute all values of k for which z' satisfies $f(z') \equiv 0 \pmod{p^{2e}}$.

   (b) Given that the only solution to $2x^3 + 4x^2 + 3 \equiv 0 \pmod{25}$ is $14 \pmod{25}$, use the lifting procedure of Part (a) to compute all the solutions of $2x^3 + 4x^2 + 3 \equiv 0 \pmod{625}$.

   [6 + 6 = 12]

5. Let g and g' be two primitive roots modulo an odd prime p. Prove that:

   (a) gg' is not a primitive root modulo p.

   (b) $g^e \pmod{p}$ is a quadratic residue modulo p if and only if e is even.

   [5 + 2 + 5 = 12]

6. Let $m \in \mathbb{N}$ be a modulus with a primitive root.

   (a) Prove that a is a primitive root modulo m if and only if $a^{\phi(m)/p} \not\equiv 1 \pmod{m}$ for every prime divisor p of $\phi(m)$.

   (b) Design an algorithm that, given $a \in \mathbb{Z}_m^*$ and the prime factorisation of $\phi(m)$ determines whether or not a is a primitive root modulo m.

   [6 + 6 = 12]

7. (a) Show that the polynomial $f(x) = x^3 + x^2 + 2$ is irreducible over $\mathbb{F}_3$.

(b) Define $\mathbb{F}_{27} = \mathbb{F}_{3^3} = \mathbb{F}_3(\theta)$ where θ is a root of $f(x)$ i.e., $\theta^3 + \theta^2 + 2 = 0$. Determine whether $\gamma = \theta + 1$ is a primitive element of $\mathbb{F}_{27}$.

Hint: $|F_{27}^{*}| = 26 = 2 \times 13$. The order of any element in $\mathbb{F}_{27}^{*}$ must be one of the following: $1, 2, 13, 26$.

(c) Is $\delta = \theta^2 \in \mathbb{F}_{27}$ a normal element of $\mathbb{F}_{27}$?

(d) Is either γ or δ primitive normal?

$\boxed{2+4+4+2 = 12}$