CS60082 Computational Number Theory, Spring 2007

Mid-semester examination

Total marks: 75 February 21, 2007 **Duration:** 2 hours

[*This test is open-notes. Answer* ***all*** *questions.*]

1 Let $m_1, m_2 \in \mathbb{N}$ with $d = \gcd(m_1, m_2)$, and let $a_1, a_2 \in \mathbb{Z}$. Consider the congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}. \end{aligned}$$

(a) First assume that $d = 1$. There exist $u, v \in \mathbb{Z}$ such that $um_1 + vm_2 = 1$. Prove that a simultaneous solution of the congruences is given by **(5)**

$$x \equiv a_1 + (a_2 - a_1)um_1 \pmod{m_1 m_2}.$$

(b) Now consider the general case $d \geqslant 1$. Prove that the given congruences are simultaneously solvable if and only if $d \mid (a_2 - a_1)$. **(8 + 2)**

(c) Prove that the solution of Part (b) is unique modulo $\operatorname{lcm}(m_1, m_2)$. **(5)**

(d) Describe an algorithm for computing this unique solution of the congruences. **(5)**

2 Let p be a prime, $p \equiv 3 \pmod 4$, and $a \in \mathbb{Z}$ with $\left(\frac{a}{p}\right) = 1$.

(a) Prove that a square root of a modulo p can be computed as $a^{(p+1)/4} \pmod p$. **(5)**

(b) How many solutions does the congruence $x^4 \equiv a \pmod p$ have? Justify your answer. **(10)**

3 Represent $\mathbb{F}_{32} = \mathbb{F}_{2^5}$ as $\mathbb{F}_2(\theta)$, where $\theta^5 + \theta^2 + 1 = 0$.

(a) Consider the two elements $\alpha = \theta^4 + \theta^2 + \theta$ and $\beta = \theta^3 + 1$ of $\mathbb{F}_{32}$ in this representation. Compute $\alpha + \beta$, $\alpha\beta$ and α/β. **(5 × 3)**

(b) Find a primitive element of $\mathbb{F}_{32}$. **(5)**

(c) Prove that $\theta + 1$ is a normal element of $\mathbb{F}_{32}$. **(5)**

4 Let γ be a primitive element of the finite field $\mathbb{F}_q$, and $r \in \mathbb{N}$. Prove that the polynomial $x^r - \gamma$ has a root in $\mathbb{F}_q$ if and only if $\gcd(r, q-1) = 1$. **(5 + 5)**

Dr. Abhijit Das, Dept. of Computer Science & Engineering, IIT Kharagpur, India