CS60082 Computational Number Theory, Spring 2007

Mid-semester examination: Solutions

---

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

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

Solution Clearly $a_1 + (a_2 - a_1)um_1 \equiv a_1 \pmod{m_1}$. Moreover, $um_1 \equiv 1 \pmod{m_2}$, so that $a_1 + (a_2 - a_1)um_1 \equiv a_1 + (a_2 - a_1) \equiv a_2 \pmod{m_2}$.

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

Solution [if] There exist $u, v \in \mathbb{Z}$ such that $um_1 + vm_2 = d$. Consider $x = a_1 + \left(\frac{a_2 - a_1}{d}\right) um_1$. Since $d \mid (a_2 - a_1)$ by hypothesis, $\left(\frac{a_2 - a_1}{d}\right)$ is an integer, so $x \equiv a_1 \pmod{m_1}$. Moreover, $um_1 = d - vm_2$, so that $a_1 + \left(\frac{a_2 - a_1}{d}\right) um_1 \equiv a_1 + (a_2 - a_1) - \left(\frac{a_2 - a_1}{d}\right) vm_2 \equiv a_2 \pmod{m_2}$. Thus $x = a_1 + \left(\frac{a_2 - a_1}{d}\right) um_1$ is a simultaneous solution of the given congruences.
[only if] Let x be a simultaneous solution of the congruences. Then for some $k_1, k_2 \in \mathbb{Z}$ we have $x = a_1 + k_1 m_1 = a_2 + k_2 m_2$, i.e., $a_2 - a_1 = k_1 m_1 - k_2 m_2$. Since $d \mid m_1$ and $d \mid m_2$, we have $d \mid (a_2 - a_1)$.

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

Solution Suppose that x, y are two solutions of the given congruences. But then $x \equiv y \pmod{m_1}$ and $x \equiv y \pmod{m_2}$, i.e., $x - y$ is a common multiple of m_1 and m_2. Therefore, $x \equiv y \pmod{\operatorname{lcm}(m_1, m_2)}$.

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

Solution By an extended gcd computation, obtain the values u, v, d satisfying $d = \gcd(m_1, m_2) = um_1 + vm_2$. Then set $x \equiv a_1 + \left(\frac{a_2 - a_1}{d}\right) um_1 \pmod{\operatorname{lcm}(m_1, m_2)}$ where $\operatorname{lcm}(m_1, m_2) = m_1 m_2 / d$.

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 $a^{(p+1)/4} \pmod p$.

Solution Let $b \equiv a^{(p+1)/4} \pmod p$. Then $b^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2} \times a \pmod p$. By Euler's criterion $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \equiv 1 \pmod p$. Therefore, $b^2 \equiv a \pmod p$.

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

Solution Let $\pm b$ be the two solutions of $y^2 \equiv a \pmod p$. The solutions of $x^4 \equiv a \pmod p$ are the solutions of $z^2 \equiv \pm b \pmod p$. Since $p \equiv 3 \pmod 4$, $\left(\frac{-1}{p}\right) = -1$. Thus if $\left(\frac{b}{p}\right) = 1$, then $\left(\frac{-b}{p}\right) = -1$, and if $\left(\frac{b}{p}\right) = -1$, then $\left(\frac{-b}{p}\right) = 1$. Therefore, exactly one of the congruences $z^2 \equiv b \pmod p$ and $z^2 \equiv -b \pmod p$ is solvable and has two solutions.
To sum up, there are exactly <u>two solutions</u> of $x^4 \equiv a \pmod p$.

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.

Solution $\alpha + \beta = \theta^4 + \theta^3 + \theta^2 + \theta + 1$.

$\alpha\beta = (\theta^4+\theta^2+\theta)(\theta^3+1) = \theta^7+\theta^4+\theta^5+\theta^2+\theta^4+\theta = \theta^7+\theta^5+\theta^2+\theta = \theta^2(\theta^2+1)+(\theta^2+1)+\theta^2+\theta = \theta^4+\theta^2+\theta^2+1+\theta^2+\theta = \theta^4+\theta^2+\theta+1$.

Since $\theta^5+\theta^2+1=0$, we have $\theta^2(\theta^3+1)=1$, i.e., $\beta^{-1}=\theta^2$. Therefore, $\alpha/\beta = \alpha\beta^{-1} = (\theta^4+\theta^2+\theta)\theta^2 = \theta^6+\theta^4+\theta^3 = \theta(\theta^2+1)+\theta^4+\theta^3 = \theta^4+\theta$.

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

Solution The size of $\mathbb{F}_{32}^*$ is 31, a prime. Thus every element of $\mathbb{F}_{32}^*$ except the identity 1 is of order 31 and is a primitive element of F_{32}.

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

Solution We have

$$\begin{aligned}
\gamma &= \theta+1,\\
\gamma^2 &= \theta^2+1,\\
\gamma^4 &= \theta^4+1,\\
\gamma^8 &= \theta^8+1 = \theta^3(\theta^2+1)+1 = \theta^5+\theta^3+1 = \theta^3+\theta^2,\\
\gamma^{16} &= \theta^6+\theta^4 = \theta(\theta^2+1)+\theta^4 = \theta^4+\theta^3+\theta.
\end{aligned}$$

Therefore, $(\gamma \quad \gamma^2 \quad \gamma^4 \quad \gamma^8 \quad \gamma^{16})^{\mathrm{t}} = T(1 \quad \theta \quad \theta^2 \quad \theta^3 \quad \theta^4)^{\mathrm{t}}$, where T is the 5×5 transformation matrix whose determinant is

$$\begin{aligned}
\begin{vmatrix} 1&1&0&0&0\\ 1&0&1&0&0\\ 1&0&0&0&1\\ 0&0&1&1&0\\ 0&1&0&1&1 \end{vmatrix}
&\equiv \begin{vmatrix} 1&0&0&0&0\\ 1&0&1&0&0\\ 1&0&0&0&1\\ 0&0&1&1&0\\ 0&1&0&1&1 \end{vmatrix} \quad \text{(adding to the topmost row all of the remaining rows)}\\
&\equiv \begin{vmatrix} 0&1&0&0\\ 0&0&0&1\\ 0&1&1&0\\ 1&0&1&1 \end{vmatrix} \quad \text{(expanding about the topmost row)}\\
&\equiv \begin{vmatrix} 1&0&0\\ 0&0&1\\ 1&1&0 \end{vmatrix} \quad \text{(expanding about the leftmost column)}\\
&\equiv \begin{vmatrix} 0&1\\ 1&0 \end{vmatrix} \quad \text{(expanding about the topmost row)}\\
&\equiv 1 \pmod 2.
\end{aligned}$$

Therefore, γ is a normal element of $\mathbb{F}_{32}$.

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 $\gcd(r,q-1)=1$.

Solution [if] We have $ur+v(q-1)=1$ for some $u,v\in\mathbb{Z}$, i.e., $(\gamma^u)^r=\gamma$, i.e., γ^u is a root of $x^r-\gamma$.

[only if] Let $\delta\in\mathbb{F}_q$ be a root of $x^r-\gamma$, i.e., $\delta^r=\gamma$. Clearly, $\delta\in\mathbb{F}_q^*$. Let $e=\operatorname{ord}\delta$. But then $q-1=\operatorname{ord}\gamma = e/\gcd(e,r)$. Moreover, $e\mid(q-1)$. So we must have $e=q-1$ and $\gcd(e,r)=1$, i.e., $\gcd(r,q-1)=1$.