Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Jose Leon

Exercise 9
- Proposed Solution -

Friday, June 24, 2016

Solution of Problem 1

Chinese Remainder Theorem:
Let $m_1, \dots, m_r$ be pair-wise relatively prime, i.e., $\gcd(m_i, m_j) = 1$ for all $i \neq j \in \{1, \dots, r\}$, and furthermore let $a_1, \dots, a_r \in \mathbb{N}$. Then, the system of congruences

$$x \equiv a_i \pmod{m_i}, \; i = 1, \dots, r,$$

has a unique solution modulo $M = \prod_{i=1}^{r} m_i$ given by

$$x \equiv \sum_{i=1}^{r} a_i M_i y_i \pmod{M}, \tag{1}$$

where $M_i = \frac{M}{m_i}$, $y_i = M_i^{-1} \pmod{m_i}$, for $i = 1, \dots, r$.

a) Show that (1) is a valid solution for the system of congruences:
Let $i \neq j \in \{1, \dots, r\}$. Since $m_j \mid M_i$ holds for all $i \neq j$, it follows:

$$M_i \equiv 0 \pmod{m_j}. \tag{2}$$

Furthermore, we have $y_j M_j \equiv 1 \pmod{m_j}$.
Note that from coprime factors of M, we obtain:

$$\gcd(M_j, m_j) = 1 \Rightarrow \exists\, y_j \equiv M_j^{-1} \pmod{m_j}, \tag{3}$$

and the solution of (1) modulo a corresponding m_j can be simplified to:

$$x \equiv \sum_{i=1}^{r} a_i M_i y_i \overset{(2)}{\equiv} a_j M_j y_j \overset{(3)}{\equiv} a_j \pmod{m_j}.$$

b) Show that the given solution is unique for the system of congruences:
Assume that two different solutions y, z exist:

$$\begin{aligned}
& y \equiv a_i \pmod{m_i} \;\wedge\; z \equiv a_i \pmod{m_i}, \; i = 1, \dots, r, \\
\Rightarrow\ & 0 \equiv (y - z) \pmod{m_i} \\
\Rightarrow\ & m_i \mid (y - z) \\
\Rightarrow\ & M \mid (y - z), \text{ as } m_1, \dots, m_r \text{ are relatively prime for } i = 1, \dots, r, \\
\Rightarrow\ & y \equiv z \pmod{M}.
\end{aligned}$$

This is a contradiction, therefore the solution is unique.

Solution of Problem 2

"$\Rightarrow$" We will show that for $n \in M$, there exists a primitive element in each case.

1) $n = 2$. This case is trivial since n is a known prime and the only element in the group $\{1\}$ is also the primitive element.
2) $n = 4 = 2^2$. In this case $\mathbb{Z}_4^* = \{1, 3\}$ and 3 is the only primitive element.
3) $n = p$. $\mathbb{Z}_p$ is a field and $\mathbb{Z}_p = \mathbb{Z}_p^*$ is a cyclic group since p is prime. Thus a primitive element exists.
4) $n = p^k$. We will show by induction, that for each odd prime p, there exists a primitive element modulo p, so that it holds for all $k > 1$:

$$\textbf{Claim 1: } g^{\varphi(p^{k-1})} \not\equiv 1 \mod p^k$$

For $k = 2$, we consider a primitive element g_0 modulo p. It holds:

$$(g_0 + p)^{p-1} \equiv g_0^{p-1} + (p-1)pg_0^{p-2} \equiv g_0^{p-1} - pg_0^{p-2} \mod p^2$$

With g_0, also $g_0 + p$ is a primitive element modulo p. Since $pg_0^{p-2} \not\equiv 0 \mod p^2$ it follows $(g_0 + p)^{p-1} \not\equiv g_0^{p-1} \mod p^2$. At most one of these numbers is kongruent to 1. We choose $g \in \{g_0, g_0 + p\}$ with $g^{p-1} \not\equiv 1 \mod p^2$ and have already proven the case $k = 2$ for Claim 1.

Next, we assume that $g^{\varphi(p^{k-1})} \not\equiv 1 \mod p^k$ holds in general and proof Claim 1 by induction for $k+1$. By Euler-Fermat it holds $g^{\varphi(p^{k-1})} \equiv 1 \mod p^{k-1}$. Hence there exists a $t \in \mathbb{Z}$ with $g^{\varphi(p^{k-1})} \equiv 1 + tp^{k-1}$. By the induction basis it holds $p \nmid t$. It follows:

$$g^{\varphi(p^k)} \equiv g^{\varphi(p^{k-1})p} \equiv (1 + tp^{k-1})^p \equiv 1 + tp^k + \binom{p}{2} t^2 p^{2k-2} \equiv 1 + tp^k \not\equiv 1 \mod p^{k+1}$$

and hence Claim 1 is proven by induction.

Next, we show that the chosen g is a primitive element modulo p^k. Let $e = \mathrm{ord}_{p^k}(g)$. From $g^e \equiv 1 \mod p^k$, if follows $g^e \equiv 1 \mod p$ and thus $p - 1 | e$. As e divides the group order of $\mathbb{Z}_{p^k}^*$ by Lagrange's Theorem, it follows that $e | \varphi(p^k) = (p-1)p^{k-1}$. There exists a $t \le k$ with $e = \varphi(p^t) = (p-1)p^{t-1}$. Due to the choice of g it follows $t = k$. Otherwise it would hold:

$$g^{\varphi(p^t)} \equiv 1 \mod p^{t+1}$$

Hence $e = \varphi(p^k)$ and it follows that $\mathbb{Z}_{p^k}^*$ is a cyclic group.

5) $n = 2p^k$. To show that $\mathbb{Z}_{2p^k}^*$ is cyclic, we choose a primitive element modulo p^k for g_0. Let g be the odd number in the set $\{g_0, g_0 + p^k\}$. We show that g is a primitive element modulo $2p^k$ (note that the even number modulo $2p^k$ is not invertible). It holds $\varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k)$. With $e = \mathrm{ord}_{2p^k}(g)$ it follows $e \mid \varphi(2p^k) = \varphi(p^k)$. Otherwise, g is a primitive element modulo p^k so that $e \ge \varphi(p^k)$ follows. Hence $e = \varphi(p^k) = \varphi(2p^k)$ and $\mathbb{Z}_{2p^k}^*$ is a cyclic group. $\square$

"$\Leftarrow$" We will show that for any $n \notin M$ it follows that $\mathbb{Z}_n^*$ is not a cyclic group. If an abelian group has more than one element of order 2, it can not be cyclic. Elements of order 2 are those square roots of 1 that differ from 1. If n has the prime factorization $\prod_i p_i^{k_i}$, it holds:

$$r^2 \equiv 1 \mod n \leftrightarrow \forall i : r^2 \equiv 1 \mod p_i^{k_i}$$

The congruence $r^2 \equiv 1 \mod p_i^{k_i}$ has for $p_i^{k_i} = 2$ exactly one and otherwise at least two solutions. With the Chinese Remainder Theorem it follows, that if at least two $p_i^{k_i} > 2$, then at least four solutions (at least three elements are of order 2. Thus the assumption follows for all $n \notin M$ that are not potences of 2. If $n = 2^k$ with $k > 2$, we show by induction over k that:

$$\textbf{Claim 2}: \forall a \in \mathbb{Z}_n^* : a^{\varphi(2^k)/2} \equiv 1 \mod 2^k$$

It follows that there is no element of order $\varphi(n)$ and thus $\mathbb{Z}_n^*$ is not cyclic. It holds $\varphi(2^k)/2 = 2^{k-1}/2 = 2^{k-2}$. For $k = 3$, we obtain $n = 8$ and $\varphi(n)/2 = 2$. It is easily computed that $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \mod 8$ is true. The induction basis $a^{2^{k-2}} \equiv 1 \mod 2^k$ provides $a^{2^{k-2}} = 1 + t2^k$ for some t. This yields:

$$a^{\varphi(2^{k+1})/2} \equiv a^{2^{k-1}} \equiv \left(a^{2^{k-2}}\right)^2 \equiv (1 + t2^k)^2 \equiv 1 + t2^{k+1} + t^2 2^{2k} \equiv 1 \mod 2^{k+1}$$

and hence Claim 2 is proven by induction.

Solution of Problem 3

a) The task is to compute $x = \log_3 y$ with $x \in \mathbb{Z}_{79}^*$ and y either 18 or 1.

- We solve $x = \log_3 18$ by an exhaustive search.

x	$3^x \mod 79$
0	1
1	3
2	9
3	27
4	$81 \equiv 2$
6	$729 \equiv 18$

$$\Rightarrow \log_3 18 \equiv 6 \mod 79$$

- We want to solve $x = \log_3 18$. From Theorem 6.2 (Euler, Fermat) we know that:

$$a^{p-1} \equiv 1 \mod 79$$

$$\Rightarrow \log_3 1 = p - 1 = 78 \mod 79$$

b) For trivial cases, $\varphi(n)$ or $\varphi(n)/2$ are the solutions. In other cases, the worst case, it would be 76 tryings. Multiplication of large numbers is computationally complex. No efficient algorithm for the calculation of the discrete logarithm is known.