Manuel Kauers
RISC-Linz

Hagenberg, December 17, 2002

Computer Algebra Exercises
Solution 4

Ex. (16) Given the problem to find a minimal $r \in \mathbb{Z}$ such that

$$r \equiv 62 \bmod 79,$$
$$r \equiv 66 \bmod 83,$$
$$r \equiv 72 \bmod 89.$$

We note that the moduli are pairwise coprime as required. To solve this problem by LAGRANGE, we first compute $((u_{kj}))_{kj}$ such that

$$1 = u_{kj} m_k + u_{jk} m_j \qquad (k \neq j)$$

using the Extended Euclidean Algorithm. We get

$$((u_{kj})) = \begin{pmatrix} * & -21 & -9 \\ 20 & * & -15 \\ 8 & 14 & * \end{pmatrix}.$$

We plug these results into

$$l_k = \prod_{\substack{j=0 \\ j \neq k}}^{2} u_{jk} m_j \bmod m_k$$

obtaining

$$l_0 = 1\,181\,920, \qquad l_1 = -2\,067\,114, \qquad l_2 = 885\,195.$$

Finally,

$$r = \sum_{k=0}^{2} r_k l_k = 62 \cdot 1\,181\,920 - 66 \cdot 2\,067\,114 + 72 \cdot 885\,195 = 583\,556.$$

Using NEWTON's algorithm, we get the same result: Denote by M_k the product of all m_i $(i < k)$ and by M_k^{-1} its inverse modulo m_k. Furthermore, let

$$s_k := ((r_k - R_k \bmod m_k) \cdot M_k^{-1}) \bmod m_k$$

and $R_k := R_{k-1} + s_k \cdot M_k$ starting with $R_0 = M_0$. Then R_2 provides the solution.

k	r_k	m_k	M_k	M_k^{-1}	s_k	R_k
0	62	79	1	1	–	62
1	66	83	79	62	82	6 540
2	72	89	6 557	46	88	583 556

Fortunately, the solution is the same.

Ex. (17) Given the problem to find a polynomial $p \in \mathbb{Q}[x]$ of minimum degree with

$$\begin{aligned} p &\equiv 7x-2 \mod x^2+x-1, \\ p &\equiv 11x+8 \mod x^2-x-1, \\ p &\equiv -3x \mod x^2+x+1. \end{aligned}$$

To find a solution via LAGRANGE, we first compute the $((u_{kj}))$ as before. There existence also proves that the moduli are coprime. We get

$$((u_{kj})) = \begin{pmatrix} * & 1/2x-1/2 & -1/2 \\ -1/2x-1/2 & * & 1/2x \\ 1/2 & -1/2x+1 & * \end{pmatrix}.$$

Plugging these results into

$$l_k = \prod_{\substack{j=0 \\ j\neq k}}^{2} u_{jk} m_j \mod m_k$$

gives

$$\begin{aligned} l_0 &= -\tfrac{1}{4}(x+1)(x^2-x-1)(x^2+x+1), \\ l_1 &= -\tfrac{1}{4}(x-1)(x^2+x-1)(x-2)(x^2+x+1), \\ l_2 &= -\tfrac{1}{4}(x^2+x-1)(x^2-x-1) \end{aligned}$$

which leads to the solution

$$p = \sum_{k=0}^{2} r_k l_k = -\tfrac{1}{4}(11x^7+x^6-36x^5-13x^4+23x^2+x-14).$$

Again, the steps of NEWTON's algorithm are presented as a table, using the same notation as in Exercise 16 above.

k	r_k	m_k	M_k	M_k^{-1}	s_k	R_k
0	$7x-2$	x^2+x-1	1	1	–	$7x-2$
1	$11x+8$	x^2-x-1	m_0	$\frac{1}{2}x-\frac{1}{2}$	$5x-3$	$5x^3+2x^2-x+1$
2	$-3x$	x^2+x+1	m_0m_1	$-\frac{1}{4}x$	x	$x^5+2x^3+2x^2+1$

In fact, MAPLE verifies that both results differ only by a multiple of $\prod_{i=0}^{2} m_i$ as they should:

```
>> p:=(x^2+x-1)*(x^2-x-1)*(x^2+x+1):
>> r:=-1/4*(11*x^7+x^6-36*x^5-13*x^4+23*x^2+x-14):
>> rem(r,p,x);
```

$$x^5+2x^3+2x^2+1$$

Ex. (18) If A_i denotes the matrix which is obtained by replacing the ith column of A by b, then CRAMER's rule says that $x = (x_1, \ldots, x_n)$ with

$$x_i = \frac{\det A_i}{\det A}$$

is a solution to $Ax = b$ if and only if $\det A = 0$ (otherwise, there is no solution).

The determinant $\det A$ may be computed modulo some primes $p_1, \ldots, p_m$, which leads to the Chinese Remainder System

$$\det A = r_i \bmod p_i \quad (i = 1, \ldots, m),$$

likewise with the determinants $\det A_i$. If the product of all the primes is larger than the value of those determinants in $\mathbb{Z}$, then the solution of those CRPs are exactly the desired values.

So, let's do it.

1. $\det A$:

$$\det A =_{19} \begin{vmatrix} 7 & 6 & 14 \\ 2 & 10 & 4 \\ 13 & 14 & 13 \end{vmatrix} =_{19} 17 + 8 + 12 - 15 - 12 - 4 =_{19} 6,$$

$$\det A =_{41} \begin{vmatrix} 7 & 6 & 36 \\ 2 & 32 & 4 \\ 13 & 36 & 35 \end{vmatrix} =_{41} 9 + 25 + 9 - 11 - 24 - 10 =_{41} 39,$$

and hence

$$\det A = 6 \bmod 19 = 39 \bmod 41.$$

which has the solution

$$\det A = 6 + 19 \cdot ((39 - 6) \cdot (19^{-1} \bmod 41) \bmod 41) = 367.$$

2. $\det A_1$:

$$\det A_1 =_{19} \begin{vmatrix} 3 & 6 & 14 \\ 5 & 10 & 4 \\ 7 & 14 & 13 \end{vmatrix} =_{19} 10 + 16 + 11 - 11 - 16 - 10 =_{19} 0,$$

$$\det A_1 =_{41} \begin{vmatrix} 3 & 6 & 36 \\ 5 & 32 & 4 \\ 7 & 36 & 35 \end{vmatrix} =_{41} 39 + 4 + 2 - 28 - 22 - 25 =_{41} 11,$$

and hence

$$\det A_1 = 0 \bmod 19 = 11 \bmod 41.$$

which has the solution

$$\det A_1 = 0 + 19 \cdot (11 \cdot (19^{-1} \bmod 41) \bmod 41) = 380.$$

3. $\det A_2$:

$$\det A_2 =_{19} \begin{vmatrix} 7 & 3 & 14 \\ 2 & 5 & 4 \\ 13 & 7 & 13 \end{vmatrix} =_{19} 18 + 4 + 6 - 17 - 6 - 2 =_{19} 3,$$

$$\det A_1 =_{41} \begin{vmatrix} 7 & 3 & 36 \\ 2 & 5 & 4 \\ 13 & 7 & 35 \end{vmatrix} =_{41} 36 + 33 + 12 - 3 - 32 - 5 =_{41} 0,$$

and hence

$$\det A_2 = 3 \bmod 19 = 0 \bmod 41.$$

which has the solution

$$\det A_2 = 3 + 19 \cdot (-3 \cdot (19^{-1} \bmod 41) \bmod 41) = 41.$$

4. $\det A_3$:

$$\det A_3 =_{19} \begin{vmatrix} 7 & 6 & 3 \\ 2 & 10 & 5 \\ 13 & 14 & 7 \end{vmatrix} =_{19} 15 + 10 + 8 - 10 - 15 - 8 =_{19} 0,$$

$$\det A_3 =_{41} \begin{vmatrix} 7 & 6 & 3 \\ 2 & 32 & 5 \\ 13 & 36 & 7 \end{vmatrix} =_{41} 10 + 21 + 11 - 18 - 30 - 2 =_{41} 33,$$

and hence

$$\det A_3 = 0 \bmod 19 = 33 \bmod 41.$$

which has the solution

$$\det A_3 = 0 + 19 \cdot (33 \cdot (19^{-1} \bmod 41) \bmod 41) = 361.$$

Putting things together, we obtain the solution

$$x = \tfrac{1}{367}(380, 41, 361) \in \mathbb{Z}^3$$

to the original system.

Ex. (19) First, Alice selects two huge primes p, q, say $p = 7$ and $q = 13$ and calculates $N = p \cdot q$ and $\varphi(N) = (p-1)(q-1)$. For security reasons, she then deletes p and q. After that she choses some $e \in \{1, \ldots, N-1\}$, say $e = 11$ and finds $d = e^{-1} \bmod \varphi(N)$ by the extended Euclidean algorithm. This is $d = 59$ in our example. She publishes $(N, e) = (91, 11)$ as her *public key* and keeps $d = 59$ private.

To send a message $m = 83$ to Alice, Bob visits her web page to find her public key $(N, e) = (91, 11)$ there. He sends

$$E(m) = m^e \bmod N = 83^{11} \bmod 91 = 34$$

to Alice.

Suppose now that Alice recieves a message $E(m) = 34$. In oder to decrypt it she calculates

$$D(E(m)) = E(m)^d \bmod N = 34^{59} \bmod 91 = 83 = m$$

because

$$E(m)^d = (m^e)^d = m^{ed} = m^{1-\varphi(N)} = m \cdot \underbrace{m^{-\varphi(N)}}_{=1 \bmod N} = m.$$

Ex. (20)

(a) To prove that $g = \gcd(m_n, M)$ is a unit, assume the contrary. Then g contains some irreducible factor $p \mid g$. By the definition of gcd, we have

$$p \mid m_n \wedge p \mid M.$$

But if $M = m_1 \cdot M'$ then by the irreducibility of p it follows that

$$p \mid m_1 \vee p \mid M'.$$

The former would contradict the fact that m_1 and m_n are coprime, and to the latter we apply the same argument iteratively until we finally get $p \mid m_{n-1}$ which is also impossible since m_{n-1} and m_n are coprime as well. $\blacksquare$.

(b) "$\Leftarrow$": Assume $r = r' \bmod m_1 m_2$. Then:

$$\begin{aligned}
& r = r' \bmod m_1 m_2 \\
\Longrightarrow \quad & m_1 m_2 \mid r - r' \\
\Longrightarrow \quad & \exists u : m_1 m_2 u = r - r' \\
\Longrightarrow \quad & \exists u_1 = u m_2 : m_1 u_1 = r - r' \wedge \exists u_2 = u m_2 : m_2 u_2 = r - r' \\
\Longrightarrow \quad & m_1 \mid r - r' \wedge m_2 \mid r - r' \\
\Longrightarrow \quad & r = r' \bmod m_1 \wedge r = r' \bmod m_2.
\end{aligned}$$

"$\Rightarrow$": Now assume $r = r' \bmod m_1$, $r = r' \bmod m_2$, and $\gcd(m_1, m_2) = 1$. Then:

$$\begin{aligned}
& r = r' \bmod m_1, \quad r = r' \bmod m_2 \\
\Longrightarrow \quad & m_1 \mid r' - r, \quad m_2 \mid r' - r \\
\Longrightarrow \quad & \exists u_1 : u_1 m_1 = r' - r \wedge \exists u_2 : u_2 m_2 = r' - r \\
\Longrightarrow \quad & u_1 m_1 = u_2 m_2 = r' - r.
\end{aligned}$$

Furthermore, we know from the coprimarity that

$$v_1 m_1 + v_2 m_2 = 1$$

for some v_1, v_2. Now,

$$\begin{aligned}
u_1 m_1 &= u_1 m_1 \cdot 1 = u_1 m_1 \cdot (v_1 m_1 + v_2 m_2) \\
&= u_1 v_1 m_1^2 + u_1 v_2 m_1 m_2 \\
&= v_1 m_1 \underbrace{(u_1 m_1)}_{= u_2 m_2} + u_1 v_2 m_1 m_2 \\
&= (v_1 u_2 + u_1 v_2) m_1 m_2,
\end{aligned}$$

and thus

$$(v_1 u_2 + u_1 v_2) m_1 m_2 = u_1 m_1 = r' - r$$

$$\begin{aligned}
\Longrightarrow \quad & m_1 m_2 \mid r' - r \\
\Longrightarrow \quad & r = r' \bmod m_1 m_2
\end{aligned}$$

which completes the proof. $\blacksquare$.