A Mechanical Proof of the Chinese Remainder Theorem

David M. Russinoff
Advanced Micro Devices, Inc.

david.russinoff@amd.com
http://www.onr.com/user/russ/david
Informal Statement

**Theorem**  Let $m_1, \ldots, m_k \in \mathbb{N}$ be pairwise relatively prime moduli and let $a_1, \ldots, a_k \in \mathbb{N}$. There exists $x \in \mathbb{N}$ such that

\[
x \equiv a_1 \pmod{m_1} \\
x \equiv a_2 \pmod{m_2} \\
\vdots \\
x \equiv a_k \pmod{m_k}.
\]

If $x'$ satisfies the same congruences, then

\[x' \equiv x \pmod{m_1 m_2 \cdots m_k}.
\]
ACL2 Formalization

(defun g-c-d (x y)  
  (declare (xargs :measure (nfix (+ x y))))  
  (if (zp x)  
    y  
    (if (zp y)  
      x  
      (if (<= x y)  
        (g-c-d x (- y x))  
        (g-c-d (- x y) y)))))

(defun rel-prime (x y)  
  (= (g-c-d x y) 1))

(defun congruent (x y m)  
  (= (rem x m) (rem y m)))

(defun congruent-all (x a m)  
  (if (endp m)  
    t  
    (and (congruent x (car a) (car m))  
      (congruent-all x (cdr a) (cdr m)))))

(defthm chinese-remainder-theorem  
  (implies (and (natp-all a)  
    (rel-prime-moduli m)  
    (= (len a) (len m)))  
    (and (natp (crt-witness a m))  
      (congruent-all (crt-witness a m) a m))))
Informal Proof

Lemma 1  If $x, y \in \mathbb{N}$ are relatively prime, then there exists $s \in \mathbb{Z}$ such that $sy \equiv 1 \pmod{x}$.

Lemma 2  If $x, y, z \in \mathbb{N}$ and $x$ is relatively prime to both $y$ and $z$, then $x$ is relatively prime to $yz$.

Proof of CRT: Let $M = m_1m_2\cdots m_k$. For $i = 1, \ldots, k$, let $M_i = M/m_i$ and find $s_i$ such that $s_iM_i \equiv 1 \pmod{m_i}$. Let

$$x = a_1s_1M_1 + a_2s_2M_2 + \cdots + a_k s_k M_k.$$ 

Then

$$x \equiv a_i s_i M_i \equiv a_i \pmod{m_i}.$$
$N \equiv 6 \pmod{25}$
Example

Suppose we have $10000 \leq N \leq 50000$ and

\[
N \equiv 6 \pmod{25}
\]
\[
N \equiv 13 \pmod{36}
\]
\[
N \equiv 28 \pmod{49}
\]

Then we may solve for $N$ as follows:

\[
M = 25 \cdot 36 \cdot 49 = 44100
\]
\[
M_1 = 36 \cdot 49 = 1764
\]
\[
M_2 = 25 \cdot 49 = 1225
\]
\[
M_3 = 25 \cdot 36 = 900
\]

\[
1764s_1 \equiv 1 \pmod{25} \iff 14s_1 \equiv 1 \pmod{25} \iff s_1 \equiv 9 \pmod{25}
\]
\[
1225s_2 \equiv 1 \pmod{36} \iff s_2 \equiv 1 \pmod{36}
\]
\[
900s_3 \equiv 1 \pmod{49} \iff 18s_3 \equiv 1 \pmod{49} \iff s_3 \equiv 30 \pmod{49}
\]

\[
a_1 = 6, \ a_2 = 13, \ a_3 = 28
\]

\[
x = a_1 M_1 s_1 + a_2 M_2 s_2 + a_3 M_3 s_3
\]
\[
= 6 \cdot 1764 \cdot 9 + 13 \cdot 1225 \cdot 1 + 28 \cdot 900 \cdot 30
\]
\[
= 867281
\]
\[
\equiv 29281 \pmod{44100}
\]

\[
N = 29281
\]
Proof of Lemma 1

Lemma 1  If \( x, y \in \mathbb{N} \) are relatively prime, then there exists \( s \in \mathbb{Z} \) such that \( sy \equiv 1 \pmod{x}. \)

This is a special case of the following:

For all \( x, y \in \mathbb{N} \), there exist \( r, s \in \mathbb{Z} \) such that \( rx + sy = \gcd(x, y). \)

The proof is by induction on \( x + y \):

(1) If \( x = 0 \), then \( r = 0 \) and \( s = 1. \)

(2) If \( y = 0 \), then \( r = 1 \) and \( s = 0. \)

(3) If \( 0 < x \leq y \), then find \( r' \) and \( s' \) such that

\[
\begin{align*}
  r'x + s'(y - x) &= \gcd(x, y - x) = \gcd(x, y) \\
  \text{and let } r &= r' - s' \text{ and } s = s'. \text{ Then} \\
  rx + sy &= (r' - s')x + s'y = r'x + s'(y - x) = \gcd(x, y).
\end{align*}
\]

(4) If \( 0 < y < x \), then find \( r' \) and \( s' \) such that

\[
\begin{align*}
  r'(x - y) + s'y &= \gcd(x - y, y) = \gcd(x, y) \\
  \text{and let } r &= r' \text{ and } s = s' - r'.
\end{align*}
\]
Formal Proof

(mutual-recursion
 (defun r (x y)
   (declare (xargs :measure (nfix (+ x y))))
   (if (zp x)
     0
     (if (zp y)
       1
       (if (<= x y)
         (- (r x (- y x)) (s x (- y x)))
         (r (- x y) y))))

(defun s (x y)
   (declare (xargs :measure (nfix (+ x y))))
   (if (zp x)
     1
     (if (zp y)
       0
       (if (<= x y)
         (s x (- y x))
         (- (s (- x y) y) (r (- x y) y))))))
)

(defun r-s-lemma
  (implies (and (natp x)
    (natp y))
    (= (+ (* (r x y) x)
        (* (s x y) y))
       (g-c-d x y))))

7
Proof of Lemma 2

Lemma 2  If \( x, y, z \in \mathbb{N} \) and \( x \) is relatively prime to both \( y \) and \( z \), then \( x \) is relatively prime to \( yz \).

This is a consequence of the following basic properties of \( \gcd \) and primes:

1. \( \gcd(x, y) \) divides both \( x \) and \( y \).
2. If \( d \) divides both \( x \) and \( y \), then \( d \) divides \( \gcd(x, y) \).
3. If \( x > 1 \), then some prime divides \( x \).
4. If a prime \( p \) divides \( ab \), then \( p \) divides either \( a \) or \( b \).

It would take some work to prove these in ACL2. Fortunately, there is a more direct route to CRT.
Alternate Approach

**Lemma 3** Let \( x, y_1, y_2, \ldots, y_k \in \mathbb{N} \) and \( p = y_1 \cdots y_k \). If \( x \) is relatively prime to each \( y_i \), then there exist \( c, d \in \mathbb{Z} \) such that \( cx + dp = 1 \).

**Proof:** Let \( p' = y_1 \cdots y_{k-1} \). Assume that

\[
x r + s y_k = 1
\]

and, by induction, that

\[
c' x + d' p' = 1.
\]

Then

\[
(sd')p = (s y_k)(d' p')
\]

\[
= (1 - r x)(1 - c' x)
\]

\[
= 1 - (r + c' - r c' x) x.
\]

Thus, if \( c = r + c' - r c' x \) and \( d = s d' \), then

\[
x c + d p = 1.
\]
Formal Proof

(defun c (x l)
  (if (endp l)
      0
      (- (+ (r x (car l))
           (c x (cdr l)))
         (* (r x (car l))
            (c x (cdr l))
            x))))

(defun d (x l)
  (if (endp l)
      1
      (* (s x (car l))
         (d x (cdr l)))))

(defun c-d-lemma
  (implies (and (natp x)
                (natp-all l)
                (rel-prime-all x l))
           (= (+ (* (c x l) x)
                  (* (d x l) (prod l)))
               1)))
Definition of \texttt{crt-witness}

\begin{verbatim}
(defun one-mod (x l)
  (* (d x 1)
      (prod 1)
      (d x 1)
      (prod 1))

(defun crt1 (a m l)
  (if (endp a)
      0
      (+ (* (car a) (one-mod (car m) (remove (car m) l)))
         (crt1 (cdr a) (cdr m) l))))

(defun crt-witness (a m) (crt1 a m m))
\end{verbatim}
The Main Lemma

We prove the following generalization of CRT:

(defthm crtl-lemma
 (implies (and (natp-all a)
               (rel-prime-moduli l)
               (sublistp m l)
               (= (len a) (len m)))
     (congruent-all (crl a m l) a m)))

The proof is by induction, as suggested by the definition:

(defun crtl (a m l)
 (if (endp a) 0
 (+ (* (car a) (one-mod (car m) (remove (car m) l)))
  (crl (cdr a) (cdr m) l))))

In the inductive case, the conclusion of the lemma expands as follows:

(and (congruent (* (car a)
                 (one-mod (car m) (remove (car m) l)))
     (crl (cdr a) (cdr m) l))
  (car a)
  (car m))
(congruent-all (* (car a)
                (one-mod (car m) (remove (car m) l)))
               (crl (cdr a) (cdr m) l))
  (cdr a)
  (cdr m))).
The Final Result

CRT is derived as an instance of \textit{crt1-lemma}:

\begin{verbatim}
(defthm crt1-lemma
 (implies (and (natp-all a)
               (rel-prime-moduli l)
               (sublistp m l)
               (= (len a) (len m)))
     (congruent-all (crt1 a m l) a m)))
\end{verbatim}

\begin{verbatim}
(defthm chinese-remainder-theorem
 (implies (and (natp-all a)
               (rel-prime-moduli m)
               (= (len a) (len m)))
     (and (natp (crt-witness a m))
          (congruent-all (crt a m) a m))))
\end{verbatim}