```
#|
 Copyright (C) 1994 by David Russinoff.  All Rights Reserved.

 You may copy and distribute verbatim copies of this Nqthm-1992 event script as
 you receive it, in any medium, including embedding it verbatim in derivative
 works, provided that you conspicuously and appropriately publish on each copy
 a valid copyright notice "Copyright (C) 1994 by David Russinoff.  All Rights
 Reserved."

 NO WARRANTY

 David Russinoff PROVIDES ABSOLUTELY NO WARRANTY.  THE EVENT SCRIPT IS
 PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED,
 INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND
 FITNESS FOR A PARTICULAR PURPOSE.  THE ENTIRE RISK AS TO THE QUALITY AND
 PERFORMANCE OF THE SCRIPT IS WITH YOU.  SHOULD THE SCRIPT PROVE DEFECTIVE, YOU
 ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

 IN NO EVENT WILL David Russinoff BE LIABLE TO YOU FOR ANY DAMAGES,
 ANY LOST PROFITS, LOST MONIES, OR OTHER SPECIAL, INCIDENTAL OR CONSEQUENTIAL
 DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THIS SCRIPT (INCLUDING BUT
 NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES
 SUSTAINED BY THIRD PARTIES), EVEN IF YOU HAVE ADVISED US OF THE POSSIBILITY OF
 SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY.

|#

; Mon Sep 17 12:10:54 CDT 1990

; This events file is an addition to the events files described in A
; Computational Logic Handbook.

; This file is a new version of the proof of Gauss's law of quadratic
; reciprocity.  It was composed entirely by David Russinoff, who also
; composed the Wilson and Gauss events in basic.events.  According to
; Russinoff, the version below is much better than the one in basic.events.
; This version also corresponds to a forthcoming paper of Russinoff in
; the Journal of Automated Reasoning.
```

EVENT: Start with the library "wilson" using the compiled version.

DEFINITION:
squares (n, p)

$=$ **if** $n \simeq \mathtt{0}$ **then** cons $(\mathtt{0},$ **nil**$)$
else cons $((n * n)$ **mod** $p,$ squares $(n - 1,\ p))$ **endif**

DEFINITION: residue $(a,\ p) = ((a$ **mod** $p) \in$ squares $(p,\ p))$

THEOREM: all-squares-1
$((p \not\simeq \mathtt{0}) \wedge (m \leq n)) \rightarrow (((m * m)$ **mod** $p) \in$ squares $(n,\ p))$

THEOREM: all-squares-2
$((y * y)$ **mod** $p) = (((y$ **mod** $p) * (y$ **mod** $p))$ **mod** $p)$

THEOREM: all-squares
$((p \not\simeq \mathtt{0}) \wedge (x \notin$ squares $(p,\ p))) \rightarrow (x \neq ((y * y)$ **mod** $p))$

THEOREM: euler-1-1
$(\neg$ divides $(\mathtt{2},\ p)) \rightarrow ((\mathtt{2} * (p \div \mathtt{2})) = (p - 1))$

THEOREM: euler-1-2
$(\neg$ divides $(\mathtt{2},\ p)) \rightarrow ($exp $(i * i,\ p \div \mathtt{2}) =$ exp $(i,\ p - 1))$

THEOREM: euler-1-3
$((a$ **mod** $p) = (b$ **mod** $p)) \rightarrow ((\exp(a,\ c)$ **mod** $p) = (\exp(b,\ c)$ **mod** $p))$

THEOREM: euler-1-4
$($prime $(p) \wedge (\neg$ divides $(\mathtt{2},\ p)) \wedge (\neg$ divides $(p,\ i)))$
$\rightarrow$ $((\exp(i * i,\ p \div \mathtt{2})$ **mod** $p) = \mathtt{1})$

THEOREM: euler-1-5
$($prime $(p) \wedge (\neg$ divides $(p,\ a)) \wedge ((a$ **mod** $p) = ((i * i)$ **mod** $p)))$
$\rightarrow$ $(\neg$ divides $(p,\ i))$

THEOREM: euler-1-6
$($prime (p)
$\wedge$ $(\neg$ divides $(\mathtt{2},\ p))$
$\wedge$ $(\neg$ divides $(p,\ a))$
$\wedge$ $((a$ **mod** $p) = ((i * i)$ **mod** $p)))$
$\rightarrow$ $((\exp(a,\ p \div \mathtt{2})$ **mod** $p) = \mathtt{1})$

THEOREM: euler-1-7
$($prime (p)
$\wedge$ $(\neg$ divides $(\mathtt{2},\ p))$
$\wedge$ $(\neg$ divides $(p,\ a))$
$\wedge$ $((a$ **mod** $p) \in$ squares $(i,\ p)))$
$\rightarrow$ $((\exp(a,\ p \div \mathtt{2})$ **mod** $p) = \mathtt{1})$

THEOREM: euler-1
$($prime $(p) \wedge (\neg$ divides $(\mathtt{2},\ p)) \wedge (\neg$ divides $(p,\ a)) \wedge$ residue $(a,\ p))$
$\rightarrow$ $((\exp(a,\ p \div \mathtt{2})$ **mod** $p) = \mathtt{1})$

DEFINITION: complement $(j,\ a,\ p) = ((\text{inverse}\,(j,\ p) * a)\ \textbf{mod}\ p)$

EVENT: Disable inverse.

THEOREM: complement-works
$(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ j)))$
$\rightarrow\quad (((j * \text{complement}\,(j,\ a,\ p))\ \textbf{mod}\ p) = (a\ \textbf{mod}\ p))$

THEOREM: bounded-complement
$(p \not\simeq \mathtt{0}) \rightarrow (\text{complement}\,(j,\ a,\ p) < p)$

EVENT: Disable complement.

THEOREM: non-zerop-complement
$(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ j)) \wedge (\neg\ \text{divides}\,(p,\ a)))$
$\rightarrow\quad (\text{complement}\,(j,\ a,\ p) \not\simeq \mathtt{0})$

THEOREM: complement-is-unique
$(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ a)) \wedge (((j * x)\ \textbf{mod}\ p) = (a\ \textbf{mod}\ p)))$
$\rightarrow\quad (\text{complement}\,(j,\ a,\ p) = (x\ \textbf{mod}\ p))$

EVENT: Disable squares.

THEOREM: no-self-complement
$(\text{prime}\,(p)$
$\wedge\quad (\neg\ \text{divides}\,(p,\ j))$
$\wedge\quad (\neg\ \text{divides}\,(p,\ a))$
$\wedge\quad (\neg\ \text{residue}\,(a,\ p)))$
$\rightarrow\quad (j \neq \text{complement}\,(j,\ a,\ p))$

THEOREM: complement-of-complement
$(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ j)) \wedge (\neg\ \text{divides}\,(p,\ a)))$
$\rightarrow\quad (\text{complement}\,(\text{complement}\,(j,\ a,\ p),\ a,\ p) = (j\ \textbf{mod}\ p))$

DEFINITION:
$\text{complements}\,(i,\ a,\ p)$
$=\quad \textbf{if}\ i \simeq \mathtt{0}\ \textbf{then nil}$
$\quad\ \textbf{elseif}\ i \in \text{complements}\,(i - 1,\ a,\ p)\ \textbf{then}\ \text{complements}\,(i - 1,\ a,\ p)$
$\quad\ \textbf{else}\ \text{cons}\,(i,\ \text{cons}\,(\text{complement}\,(i,\ a,\ p),\ \text{complements}\,(i - 1,\ a,\ p)))\ \textbf{endif}$

THEOREM: all-non-zerop-complements
$(\text{prime}\,(p) \wedge (i < p) \wedge (\neg\ \text{divides}\,(p,\ a)))$
$\rightarrow\quad \text{all-non-zerop}\,(\text{complements}\,(i,\ a,\ p))$

THEOREM: bounded-complements
$(i < p) \rightarrow \text{all-lesseqp}\,(\text{complements}\,(i,\ a,\ p),\ p - 1)$

THEOREM: subsetp-positives-complements
$\text{subsetp}\,(\text{positives}\,(n),\ \text{complements}\,(n,\ a,\ p))$

THEOREM: complements-closed-1
$(\text{prime}\,(p)$
$\wedge\quad (i \not\simeq \mathtt{0})$
$\wedge\quad (i < p)$
$\wedge\quad (\neg\ \text{divides}\,(p,\ a))$
$\wedge\quad (j \in \text{complements}\,(i,\ a,\ p)))$
$\rightarrow\quad (\text{complement}\,(j,\ a,\ p) \in \text{complements}\,(i,\ a,\ p))$

THEOREM: complements-closed-2
$(\text{prime}\,(p)$
$\wedge\quad (i \not\simeq \mathtt{0})$
$\wedge\quad (j \not\simeq \mathtt{0})$
$\wedge\quad (i < p)$
$\wedge\quad (j < p)$
$\wedge\quad (\neg\ \text{divides}\,(p,\ a))$
$\wedge\quad (\text{complement}\,(j,\ a,\ p) \in \text{complements}\,(i,\ a,\ p)))$
$\rightarrow\quad (j \in \text{complements}\,(i,\ a,\ p))$

THEOREM: all-distinct-complements-1
$(\text{prime}\,(p)$
$\wedge\quad (i < p)$
$\wedge\quad (\neg\ \text{divides}\,(p,\ a))$
$\wedge\quad (\neg\ \text{residue}\,(a,\ p))$
$\wedge\quad \text{all-distinct}\,(\text{complements}\,(i - 1,\ a,\ p)))$
$\rightarrow\quad \text{all-distinct}\,(\text{complements}\,(i,\ a,\ p))$

THEOREM: all-distinct-complements
$(\text{prime}\,(p) \wedge (i < p) \wedge (\neg\ \text{divides}\,(p,\ a)) \wedge (\neg\ \text{residue}\,(a,\ p)))$
$\rightarrow\quad \text{all-distinct}\,(\text{complements}\,(i,\ a,\ p))$

THEOREM: perm-positives-complements
$(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ a)) \wedge (\neg\ \text{residue}\,(a,\ p)))$
$\rightarrow\quad \text{perm}\,(\text{positives}\,(p - 1),\ \text{complements}\,(p - 1,\ a,\ p))$

THEOREM: complements-fact
$(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ a)) \wedge (\neg\ \text{residue}\,(a,\ p)))$
$\rightarrow\quad (\text{times-list}\,(\text{complements}\,(p - 1,\ a,\ p)) = \text{fact}\,(p - 1))$

THEOREM: times-mod-4
$(((i * j)\ \mathbf{mod}\ p) = (a\ \mathbf{mod}\ p))$
$\rightarrow\quad (((i * (j * k))\ \mathbf{mod}\ p) = ((a * (k\ \mathbf{mod}\ p))\ \mathbf{mod}\ p))$

THEOREM: times-complements-1
$((((i * \text{complement}\,(i,\ a,\ p))\ \textbf{mod}\ p) = (a\ \textbf{mod}\ p))$
$\wedge\quad ((i \not\simeq 0) \wedge (i \notin \text{complements}\,(i-1,\ a,\ p))))$
$\rightarrow\quad ((\text{times-list}\,(\text{complements}\,(i,\ a,\ p))\ \textbf{mod}\ p)$
$=\quad ((a * (\text{times-list}\,(\text{complements}\,(i-1,\ a,\ p))\ \textbf{mod}\ p))\ \textbf{mod}\ p))$

THEOREM: times-complements-2
$(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ i)) \wedge (i \notin \text{complements}\,(i-1,\ a,\ p)))$
$\rightarrow\quad ((\text{times-list}\,(\text{complements}\,(i,\ a,\ p))\ \textbf{mod}\ p)$
$=\quad ((a * (\text{times-list}\,(\text{complements}\,(i-1,\ a,\ p))\ \textbf{mod}\ p))\ \textbf{mod}\ p))$

THEOREM: quotient-plus-1
$((n \not\simeq 0) \wedge (x \in \mathbf{N}) \wedge (y = (x + n)))$
$\rightarrow\quad ((y \div n) = (1 + (x \div n)))$

THEOREM: times-complements-3
$((i \not\simeq 0) \wedge (i \notin \text{complements}\,(i-1,\ a,\ p)))$
$\rightarrow\quad ((\text{length}\,(\text{complements}\,(i,\ a,\ p)) \div 2)$
$=\quad (1 + (\text{length}\,(\text{complements}\,(i-1,\ a,\ p)) \div 2)))$

THEOREM: times-complements-4
$(\text{prime}\,(p)$
$\wedge\quad (i \not\simeq 0)$
$\wedge\quad (i < p)$
$\wedge\quad ((\text{times-list}\,(\text{complements}\,(i-1,\ a,\ p))\ \textbf{mod}\ p)$
$=\quad (\exp\,(a,\ \text{length}\,(\text{complements}\,(i-1,\ a,\ p)) \div 2)\ \textbf{mod}\ p)))$
$\rightarrow\quad ((\text{times-list}\,(\text{complements}\,(i,\ a,\ p))\ \textbf{mod}\ p)$
$=\quad (\exp\,(a,\ \text{length}\,(\text{complements}\,(i,\ a,\ p)) \div 2)\ \textbf{mod}\ p))$

THEOREM: times-complements-5
$(i \simeq 0)$
$\rightarrow\quad ((\text{times-list}\,(\text{complements}\,(i,\ a,\ p))\ \textbf{mod}\ p)$
$=\quad (\exp\,(a,\ \text{length}\,(\text{complements}\,(i,\ a,\ p)) \div 2)\ \textbf{mod}\ p))$

THEOREM: times-complements
$(\text{prime}\,(p) \wedge (i < p))$
$\rightarrow\quad ((\text{times-list}\,(\text{complements}\,(i,\ a,\ p))\ \textbf{mod}\ p)$
$=\quad (\exp\,(a,\ \text{length}\,(\text{complements}\,(i,\ a,\ p)) \div 2)\ \textbf{mod}\ p))$

THEOREM: sub1-length-delete
$(x \in b) \rightarrow (\text{length}\,(\text{delete}\,(x,\ b)) = (\text{length}\,(b) - 1))$

THEOREM: equal-length-perm
$\text{perm}\,(a,\ b) \rightarrow (\text{length}\,(a) = \text{length}\,(b))$

THEOREM: length-positives
$\text{length}\,(\text{positives}\,(n)) = \text{fix}\,(n)$

THEOREM: euler-2-1
$(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ a)) \wedge (\neg\ \text{residue}\,(a,\ p)))$
$\rightarrow\quad ((\exp\,(a,\ \text{length}\,(\text{complements}\,(p-1,\ a,\ p)) \div \mathtt{2})\ \textbf{mod}\ p) = (p-1))$

THEOREM: euler-2-2
$(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ a)) \wedge (\neg\ \text{residue}\,(a,\ p)))$
$\rightarrow\quad (\text{length}\,(\text{complements}\,(p-1,\ a,\ p)) = (p-1))$

THEOREM: euler-2-3
$(p \not\simeq \mathtt{0}) \rightarrow (\text{divides}\,(\mathtt{2},\ p) = (\neg\ \text{divides}\,(\mathtt{2},\ p-1)))$

THEOREM: euler-2-4
$(\neg\ \text{divides}\,(\mathtt{2},\ p)) \rightarrow (((p-1) \div \mathtt{2}) = (p \div \mathtt{2}))$

THEOREM: euler-2
$\text{prime}\,(p)$
$\wedge\quad (\neg\ \text{divides}\,(\mathtt{2},\ p))$
$\wedge\quad (\neg\ \text{divides}\,(p,\ a))$
$\wedge\quad (\neg\ \text{residue}\,(a,\ p)))$
$\rightarrow\quad ((\exp\,(a,\ p \div \mathtt{2})\ \textbf{mod}\ p) = (p-1))$

DEFINITION:
$\text{evenp}\,(x)$
$=\quad \textbf{if}\ x \simeq \mathtt{0}\ \textbf{then t}$
$\quad\ \ \textbf{else}\ \neg\ \text{evenp}\,(x-1)\ \textbf{endif}$

THEOREM: evenp-plus
$\text{evenp}\,(a+b) = (\text{evenp}\,(a) = \text{evenp}\,(b))$

THEOREM: evenp-diff
$\text{evenp}\,(p-x) = ((p < x) \vee (\text{evenp}\,(p) = \text{evenp}\,(x)))$

THEOREM: evenp-times
$\text{evenp}\,(a * b) = (\text{evenp}\,(a) \vee \text{evenp}\,(b))$

THEOREM: evenp-even
$\text{even}\,(p) = \text{evenp}\,(p)$

THEOREM: even-plus
$\text{even}\,(a+b) = (\text{even}\,(a) = \text{even}\,(b))$

THEOREM: even-diff
$\text{even}\,(p-x) = ((p < x) \vee (\text{even}\,(p) = \text{even}\,(x)))$

THEOREM: even-times
$\text{even}\,(a * b) = (\text{even}\,(a) \vee \text{even}\,(b))$

THEOREM: even-rem
$(\neg \text{ even}\,(p)) \rightarrow (\text{even}\,(p - (x \textbf{ mod } p)) = (\neg \text{ even}\,(x \textbf{ mod } p)))$

THEOREM: even-add1
$\text{even}\,(1 + x) = (\neg \text{ even}\,(x))$

EVENT: Disable evenp-even.

THEOREM: even-prime-2
$(\text{prime}\,(p) \wedge (p \neq \mathtt{2})) \rightarrow (\neg \text{ even}\,(p))$

THEOREM: even-prime
$(\text{prime}\,(p) \wedge (p \neq \mathtt{2})) \rightarrow ((p \textbf{ mod } \mathtt{2}) \neq \mathtt{0})$

THEOREM: euler-criterion
$(\text{prime}\,(p) \wedge (p \neq \mathtt{2}) \wedge (\neg \text{ divides}\,(p,\ a)))$
$\rightarrow \quad ((\exp\,(a,\ p \div \mathtt{2}) \textbf{ mod } p)$
$= \quad \textbf{if } \text{residue}\,(a,\ p) \textbf{ then } \mathtt{1}$
$\textbf{else } p - 1 \textbf{ endif})$

EVENT: Disable euler-1.

EVENT: Disable euler-2.

DEFINITION:
$\text{res1}\,(n,\ a,\ p)$
$= \quad \textbf{if } n \simeq \mathtt{0} \textbf{ then t}$
$\textbf{elseif } (p \div \mathtt{2}) < ((a * n) \textbf{ mod } p) \textbf{ then } \neg \text{ res1}\,(n - 1,\ a,\ p)$
$\textbf{else } \text{res1}\,(n - 1,\ a,\ p) \textbf{ endif}$

DEFINITION:
$\text{reflections}\,(n,\ a,\ p)$
$= \quad \textbf{if } n \simeq \mathtt{0} \textbf{ then nil}$
$\textbf{elseif } (p \div \mathtt{2}) < ((a * n) \textbf{ mod } p)$
$\textbf{then } \text{cons}\,(p - ((a * n) \textbf{ mod } p), \text{reflections}\,(n - 1,\ a,\ p))$
$\textbf{else } \text{cons}\,((a * n) \textbf{ mod } p, \text{reflections}\,(n - 1,\ a,\ p)) \textbf{ endif}$

THEOREM: diff-mod-1
$(b \leq a) \rightarrow (((a - (b \textbf{ mod } p)) \textbf{ mod } p) = ((a - b) \textbf{ mod } p))$

THEOREM: rem-diff-times
$((x < p) \wedge ((x \not\simeq \mathtt{0}) \wedge (b \not\simeq \mathtt{0})))$
$\rightarrow \quad ((((b * p) - x) \textbf{ mod } p) = (p - x))$

THEOREM: reflect-commutes-with-times-1
$(y \leq p)$
$\rightarrow \quad ((((p - y) * x) \textbf{ mod } p) = ((p - ((y * x) \textbf{ mod } p)) \textbf{ mod } p))$

THEOREM: reflect-commutes-with-times-2
$(y \leq p)$
$\rightarrow \quad (((x * (p - y)) \textbf{ mod } p) = ((p - ((x * y) \textbf{ mod } p)) \textbf{ mod } p))$

THEOREM: times-exp-fact
$(n \not\simeq 0)$
$\rightarrow \quad ((((a * n) * (\exp(a,\ n - 1) * \text{fact}(n - 1))) \textbf{ mod } p)$
$\quad = \quad ((\exp(a,\ n) * \text{fact}(n)) \textbf{ mod } p))$

THEOREM: rem-reflections-1
$((p \not\simeq 0)$
$\wedge \quad (n \not\simeq 0)$
$\wedge \quad ((p \div 2) \not< ((a * n) \textbf{ mod } p))$
$\wedge \quad ((\text{times-list}(\text{reflections}(n - 1,\ a,\ p)) \textbf{ mod } p)$
$\quad = \quad ((\exp(a,\ n - 1) * \text{fact}(n - 1)) \textbf{ mod } p)))$
$\rightarrow \quad ((\text{times-list}(\text{reflections}(n,\ a,\ p)) \textbf{ mod } p)$
$\quad = \quad ((\exp(a,\ n) * \text{fact}(n)) \textbf{ mod } p))$

THEOREM: rem-reflections-2
$((p \not\simeq 0)$
$\wedge \quad (n \not\simeq 0)$
$\wedge \quad ((p \div 2) < ((a * n) \textbf{ mod } p))$
$\wedge \quad ((\text{times-list}(\text{reflections}(n - 1,\ a,\ p)) \textbf{ mod } p)$
$\quad = \quad ((\exp(a,\ n - 1) * \text{fact}(n - 1)) \textbf{ mod } p)))$
$\rightarrow \quad ((\text{times-list}(\text{reflections}(n,\ a,\ p)) \textbf{ mod } p)$
$\quad = \quad ((p - ((\exp(a,\ n) * \text{fact}(n)) \textbf{ mod } p)) \textbf{ mod } p))$

THEOREM: rem-reflections-3
$((p \not\simeq 0)$
$\wedge \quad (n \not\simeq 0)$
$\wedge \quad (((a * n) \textbf{ mod } p) \leq (p \div 2))$
$\wedge \quad ((\text{times-list}(\text{reflections}(n - 1,\ a,\ p)) \textbf{ mod } p)$
$\quad = \quad ((p - ((\exp(a,\ n - 1) * \text{fact}(n - 1)) \textbf{ mod } p)) \textbf{ mod } p)))$
$\rightarrow \quad ((\text{times-list}(\text{reflections}(n,\ a,\ p)) \textbf{ mod } p)$
$\quad = \quad ((p - ((\exp(a,\ n) * \text{fact}(n)) \textbf{ mod } p)) \textbf{ mod } p))$

THEOREM: double-reflect
$(a \leq p) \rightarrow (((p - ((p - a) \textbf{ mod } p)) \textbf{ mod } p) = (a \textbf{ mod } p))$

THEOREM: rem-reflections-4
$((p \not\simeq 0)$

$\wedge \quad (n \not\simeq 0)$
$\wedge \quad ((p \div 2) < ((a * n) \bmod p))$
$\wedge \quad ((\text{times-list}\,(\text{reflections}\,(n-1,\ a,\ p)) \bmod p)$
$\quad\quad = \quad ((p - ((\exp(a,\ n-1) * \text{fact}\,(n-1)) \bmod p)) \bmod p)))$
$\rightarrow \quad ((\text{times-list}\,(\text{reflections}\,(n,\ a,\ p)) \bmod p)$
$\quad\quad = \quad ((\exp(a,\ n) * \text{fact}\,(n)) \bmod p))$

THEOREM: rem-reflections-base-case
$(n \simeq 0)$
$\rightarrow \quad ((\text{times-list}\,(\text{reflections}\,(n,\ a,\ p)) \bmod p)$
$\quad\quad = \quad ((\exp(a,\ n) * \text{fact}\,(n)) \bmod p))$

THEOREM: rem-reflections
$(p \not\simeq 0)$
$\rightarrow \quad ((\text{times-list}\,(\text{reflections}\,(n,\ a,\ p)) \bmod p)$
$\quad\quad = \quad \textbf{if}\ \text{res1}\,(n,\ a,\ p)\ \textbf{then}\ (\exp(a,\ n) * \text{fact}\,(n)) \bmod p$
$\quad\quad\quad\quad \textbf{else}\ (p - ((\exp(a,\ n) * \text{fact}\,(n)) \bmod p)) \bmod p\ \textbf{endif})$

THEOREM: length-reflections
$\text{length}\,(\text{reflections}\,(n,\ a,\ p)) = \text{fix}\,(n)$

THEOREM: all-lesseqp-reflections-1
$((p \div 2) < x) \rightarrow ((p \div 2) \not< (p - x))$

THEOREM: all-lesseqp-reflections
$\text{all-lesseqp}\,(\text{reflections}\,(n,\ a,\ p),\ p \div 2)$

THEOREM: all-non-zerop-reflections
$(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ a)) \wedge (b < p))$
$\rightarrow \quad \text{all-non-zerop}\,(\text{reflections}\,(b,\ a,\ p))$

THEOREM: all-distinct-reflections-1
$(\text{prime}\,(p) \wedge (j < i) \wedge (i < p) \wedge (\neg\ \text{divides}\,(p,\ a)))$
$\rightarrow \quad (((a * i) \bmod p) \neq ((a * j) \bmod p))$

THEOREM: all-distinct-reflections-2
$((x \in \mathbf{N}) \wedge (y \in \mathbf{N}) \wedge (x < p) \wedge (y < p))$
$\rightarrow \quad (((p - x) = (p - y)) = (x = y))$

THEOREM: numberp-remainder
$(a \bmod p) \in \mathbf{N}$

THEOREM: all-distinct-reflections-3
$(\text{prime}\,(p) \wedge (j < i) \wedge (i < p) \wedge (\neg\ \text{divides}\,(p,\ a)))$
$\rightarrow \quad ((p - ((a * i) \bmod p)) \neq (p - ((a * j) \bmod p)))$

THEOREM: plus-mod-1
$(((x \textbf{ mod } p) + y) \textbf{ mod } p) = ((x + y) \textbf{ mod } p)$

THEOREM: plus-mod-2
$((y + (x \textbf{ mod } p)) \textbf{ mod } p) = ((x + y) \textbf{ mod } p)$

THEOREM: all-distinct-reflections-4
$((x = (p - y)) \wedge (y < p)) \rightarrow (((x + y) \textbf{ mod } p) = \texttt{'0})$

THEOREM: all-distinct-reflections-5
$((((a * i) \textbf{ mod } p) = (p - ((a * j) \textbf{ mod } p))) \wedge (p \not\simeq \texttt{0}))$
$\rightarrow \quad (((a * (i + j)) \textbf{ mod } p) = \texttt{'0})$

THEOREM: all-distinct-reflections-6
$((i \leq (p \div \texttt{2})) \wedge (j < i))$
$\rightarrow \quad (((i + j) \not\simeq \texttt{0}) \wedge ((i + j) < p))$

THEOREM: all-distinct-reflections-7
$(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ a)) \wedge (i \leq (p \div \texttt{2})) \wedge (j < i))$
$\rightarrow \quad (((a * i) \textbf{ mod } p) \neq (p - ((a * j) \textbf{ mod } p)))$

THEOREM: all-distinct-reflections-8
$(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ a)) \wedge (i \leq (p \div \texttt{2})) \wedge (j < i))$
$\rightarrow \quad ((p - ((a * i) \textbf{ mod } p)) \neq ((a * j) \textbf{ mod } p))$

THEOREM: all-distinct-reflections-9
$(\text{prime}\,(p)$
$\wedge \quad (\neg\ \text{divides}\,(\texttt{2},\ p))$
$\wedge \quad (\neg\ \text{divides}\,(p,\ a))$
$\wedge \quad (i \leq (p \div \texttt{2}))$
$\wedge \quad (j < i))$
$\rightarrow \quad (((a * i) \textbf{ mod } p) \notin \text{reflections}\,(j,\ a,\ p))$

THEOREM: all-distinct-reflections-10
$(\text{prime}\,(p)$
$\wedge \quad (\neg\ \text{divides}\,(\texttt{2},\ p))$
$\wedge \quad (\neg\ \text{divides}\,(p,\ a))$
$\wedge \quad (i \leq (p \div \texttt{2}))$
$\wedge \quad (j < i))$
$\rightarrow \quad ((p - ((a * i) \textbf{ mod } p)) \notin \text{reflections}\,(j,\ a,\ p))$

THEOREM: all-distinct-reflections
$(\text{prime}\,(p)$
$\wedge \quad (\neg\ \text{divides}\,(\texttt{2},\ p))$
$\wedge \quad (\neg\ \text{divides}\,(p,\ a))$
$\wedge \quad (i \leq (p \div \texttt{2})))$
$\rightarrow \quad \text{all-distinct}\,(\text{reflections}\,(i,\ a,\ p))$

THEOREM: times-reflections
(prime (*p*) ∧ (¬ divides (2, *p*)) ∧ (¬ divides (*p*, *a*)))
→ (times-list (reflections (*p* ÷ 2, *a*, *p*)) = fact (*p* ÷ 2))

THEOREM: plus-x-x-even
((*x* + *x*) **mod** 2) = '0

THEOREM: res1-rem-1-1
((*x* ≠ 0) ∧ (¬ divides (2, *p*))) → (((*p* − *x*) **mod** *p*) ≠ *x*)

THEOREM: res1-rem-1
(prime (*p*)
∧ (¬ divides (2, *p*))
∧ (¬ divides (*p*, *a*))
∧ res1 (*p* ÷ 2, *a*, *p*))
→ ((exp (*a*, *p* ÷ 2) **mod** *p*) = 1)

THEOREM: remainder-lessp
(*a* < *p*) → ((*a* **mod** *p*) = fix (*a*))

THEOREM: res1-rem-2
(prime (*p*)
∧ (¬ divides (2, *p*))
∧ (¬ divides (*p*, *a*))
∧ (¬ res1 (*p* ÷ 2, *a*, *p*)))
→ ((exp (*a*, *p* ÷ 2) **mod** *p*) ≠ 1)

THEOREM: two-even
(¬ divides (2, *p*)) → ((*p* − 1) ≠ 1)

THEOREM: perm-reflections
(prime (*p*) ∧ (*p* ≠ 2) ∧ (¬ divides (*p*, *a*)))
→ perm (positives (*p* ÷ 2), reflections (*p* ÷ 2, *a*, *p*))

THEOREM: gauss-lemma-lemma
(prime (*p*) ∧ (¬ divides (*p*, *a*)) ∧ (¬ divides (2, *p*)))
→ (res1 (*p* ÷ 2, *a*, *p*) = residue (*a*, *p*))

DEFINITION:
mu (*n*, *a*, *p*)
= **if** *n* ≃ 0 **then t**
elseif (*p* ÷ 2) < ((*a* ∗ *n*) **mod** *p*) **then** 1 + mu (*n* − 1, *a*, *p*)
else mu (*n* − 1, *a*, *p*) **endif**

DEFINITION: gauss (*a*, *p*) = even (mu (*p* ÷ 2, *a*, *p*))

THEOREM: res1-gauss
res1 $(n,\ a,\ p) = \text{even}\,(\text{mu}\,(n,\ a,\ p))$

THEOREM: gauss-lemma
$(\text{prime}\,(p) \wedge (p \neq 2) \wedge (\neg\ \text{divides}\,(p,\ a)))$
$\rightarrow\quad (\text{gauss}\,(a,\ p) = \text{residue}\,(a,\ p))$

DEFINITION:
sum (l)
$=\quad$ **if** listp (l) **then** car (l) + sum (cdr (l))
else 0 **endif**

DEFINITION:
quotients $(n,\ a,\ p)$
$=\quad$ **if** $n \simeq 0$ **then nil**
else cons $((a * n) \div p,$ quotients $(n - 1,\ a,\ p))$ **endif**

DEFINITION:
remainders $(n,\ a,\ p)$
$=\quad$ **if** $n \simeq 0$ **then nil**
else cons $((a * n)$ **mod** $p,$ remainders $(n - 1,\ a,\ p))$ **endif**

THEOREM: quotient-remainder-sum
$(a * \text{sum}\,(\text{positives}\,(n)))$
$=\quad ((p * \text{sum}\,(\text{quotients}\,(n,\ a,\ p))) + \text{sum}\,(\text{remainders}\,(n,\ a,\ p)))$

THEOREM: quotient-remainder-sum-parity
$\text{even}\,(a * \text{sum}\,(\text{positives}\,(n)))$
$=\quad \text{even}\,((p * \text{sum}\,(\text{quotients}\,(n,\ a,\ p))) + \text{sum}\,(\text{remainders}\,(n,\ a,\ p)))$

THEOREM: even-mu
$(\neg\ \text{even}\,(p))$
$\rightarrow\quad (\text{even}\,(\text{mu}\,(n,\ a,\ p))$
$=\quad (\text{even}\,(\text{sum}\,(\text{remainders}\,(n,\ a,\ p)))$
$\leftrightarrow\quad \text{even}\,(\text{sum}\,(\text{reflections}\,(n,\ a,\ p)))))$

THEOREM: perm-sum-lemma
$(x \in m) \rightarrow ((x + \text{sum}\,(\text{delete}\,(x,\ m))) = \text{sum}\,(m))$

THEOREM: perm-sum
$\text{perm}\,(l,\ m) \rightarrow (\text{sum}\,(l) = \text{sum}\,(m))$

THEOREM: sum-reflections
$(\text{prime}\,(p) \wedge (p \neq 2) \wedge (\neg\ \text{divides}\,(p,\ a)))$
$\rightarrow\quad (\text{sum}\,(\text{reflections}\,(p \div 2,\ a,\ p)) = \text{sum}\,(\text{positives}\,(p \div 2)))$

THEOREM: gauss-quotients
$(\text{prime}\,(p) \wedge (p \neq \mathtt{2}) \wedge (\neg\ \text{even}\,(a)) \wedge (\neg\ \text{divides}\,(p,\ a)))$
$\rightarrow\quad (\text{gauss}\,(a,\ p) = \text{even}\,(\text{sum}\,(\text{quotients}\,(p \div \mathtt{2},\ a,\ p))))$

THEOREM: equal-residue-even-plus
$(\text{prime}\,(p) \wedge (p \neq \mathtt{2}) \wedge \text{prime}\,(q) \wedge (q \neq \mathtt{2}) \wedge (p \neq q))$
$\rightarrow\quad ((\text{residue}\,(q,\ p) = \text{residue}\,(p,\ q))$
$\quad = \quad \text{even}\,(\text{sum}\,(\text{quotients}\,(p \div \mathtt{2},\ q,\ p))$
$\quad\quad + \quad \text{sum}\,(\text{quotients}\,(q \div \mathtt{2},\ p,\ q))))$

DEFINITION:
$\text{w}\,(x,\ l)$
$=\quad$ **if** $\text{listp}\,(l)$
then if $\text{car}\,(l) < x$ **then** $1 + \text{w}\,(x,\ \text{cdr}\,(l))$
else $\text{w}\,(x,\ \text{cdr}\,(l))$ **endif**
else $\mathtt{0}$ **endif**

DEFINITION:
$\text{wins}\,(k,\ l)$
$=\quad$ **if** $\text{listp}\,(k)$ **then** $\text{w}\,(\text{car}\,(k),\ l) + \text{wins}\,(\text{cdr}\,(k),\ l)$
else $\mathtt{0}$ **endif**

DEFINITION:
$\text{all-numberp}\,(l)$
$=\quad$ **if** $\text{listp}\,(l)$ **then** $(\text{car}\,(l) \in \mathbf{N}) \wedge \text{all-numberp}\,(\text{cdr}\,(l))$
else t endif

DEFINITION:
$\text{l}\,(x,\ l)$
$=\quad$ **if** $\text{listp}\,(l)$
then if $x < \text{car}\,(l)$ **then** $1 + \text{l}\,(x,\ \text{cdr}\,(l))$
else $\text{l}\,(x,\ \text{cdr}\,(l))$ **endif**
else $\mathtt{0}$ **endif**

DEFINITION:
$\text{losses}\,(k,\ l)$
$=\quad$ **if** $\text{listp}\,(k)$ **then** $\text{l}\,(\text{car}\,(k),\ l) + \text{losses}\,(\text{cdr}\,(k),\ l)$
else $\mathtt{0}$ **endif**

THEOREM: plus-l-w
$((x \notin l) \wedge (x \in \mathbf{N}) \wedge \text{all-numberp}\,(l))$
$\rightarrow\quad ((\text{l}\,(x,\ l) + \text{w}\,(x,\ l)) = \text{length}\,(l))$

THEOREM: plus-wins-losses
$((\text{intersect}\,(l,\ m) \simeq \mathbf{nil}) \wedge \text{all-numberp}\,(l) \wedge \text{all-numberp}\,(m))$
$\rightarrow\quad ((\text{wins}\,(l,\ m) + \text{losses}\,(l,\ m)) = (\text{length}\,(l) * \text{length}\,(m)))$

THEOREM: equal-wins-losses
$\text{losses}\,(l,\ m) = \text{wins}\,(m,\ l)$

THEOREM: plus-wins-wins
$((\text{intersect}\,(l,\ m) \simeq \textbf{nil}) \wedge \text{all-numberp}\,(l) \wedge \text{all-numberp}\,(m))$
$\rightarrow \quad ((\text{wins}\,(l,\ m) + \text{wins}\,(m,\ l)) = (\text{length}\,(l) * \text{length}\,(m)))$

DEFINITION:
$\text{mults}\,(n,\ p)$
$= \quad \textbf{if } n \simeq \mathtt{0} \textbf{ then nil}$
$\quad\ \textbf{else } \text{cons}\,(n * p,\ \text{mults}\,(n - 1,\ p))\ \textbf{endif}$

THEOREM: all-numberp-mults
$(p \not\simeq \mathtt{0}) \rightarrow \text{all-numberp}\,(\text{mults}\,(n,\ p))$

THEOREM: empty-intersect-mults-lemma
$(\text{prime}\,(p) \wedge \text{prime}\,(q) \wedge (p \neq q) \wedge (i < q) \wedge (j < p))$
$\rightarrow \quad ((i * p) \notin \text{mults}\,(j,\ q))$

THEOREM: empty-intersect-mults
$(\text{prime}\,(p) \wedge \text{prime}\,(q) \wedge (p \neq q) \wedge (i < q))$
$\rightarrow \quad (\neg\ \text{listp}\,(\text{intersect}\,(\text{mults}\,(i,\ p),\ \text{mults}\,(p \div \mathtt{2},\ q))))$

THEOREM: length-mults
$(n \in \mathbf{N}) \rightarrow (\text{length}\,(\text{mults}\,(n,\ p)) = n)$

THEOREM: lessp-a
$(p \not\simeq \mathtt{0}) \rightarrow (a < ((1 + (a \div p)) * p))$

THEOREM: leq-w-n
$n \not< \text{w}\,(a,\ \text{mults}\,(n,\ p))$

THEOREM: lessp-rewrite
$((a < (m * p)) \wedge (m \leq n)) \rightarrow (a < (n * p))$

THEOREM: lessp-w-m
$(a < (m * p)) \rightarrow (\text{w}\,(a,\ \text{mults}\,(n,\ p)) < m)$

THEOREM: leq-w-quotient
$(p \not\simeq \mathtt{0}) \rightarrow (\text{w}\,(a,\ \text{mults}\,(n,\ p)) \leq (a \div p))$

THEOREM: monotone-w
$(m \leq n) \rightarrow (\text{w}\,(a,\ \text{mults}\,(m,\ p)) \leq \text{w}\,(a,\ \text{mults}\,(n,\ p)))$

THEOREM: leq-n-w
$((n * p) < a) \rightarrow (n \leq \text{w}\,(a,\ \text{mults}\,(n,\ p)))$

THEOREM: leq-quotient-w
$((p \not\simeq 0) \wedge (\neg\, \text{divides}\,(p,\, a)) \wedge ((a \div p) \leq n))$
$\rightarrow \quad ((a \div p) \leq \text{w}\,(a, \text{mults}\,(n,\, p)))$

DEFINITION:
lqq-induct $(a,\, b,\, c,\, d)$
$=$ **if** $b \simeq 0$ **then t**
elseif $d \simeq 0$ **then t**
elseif $a < d$ **then t**
elseif $c < b$ **then t**
else lqq-induct $(a - d,\, b,\, c - b,\, d)$ **endif**

THEOREM: leq-times-quot
$((b \not\simeq 0) \wedge ((a * b) \leq (c * d))) \rightarrow ((a \div d) \leq (c \div b))$

THEOREM: leq-j-a
$(j \leq a) \rightarrow ((j * q) \leq (a * q))$

THEOREM: leq-quot-times
$(j \leq (p \div 2)) \rightarrow (((j * q) \div p) \leq (q \div 2))$

THEOREM: equal-quot-w
$(\text{prime}\,(p) \wedge (\neg\, \text{divides}\,(p,\, q)) \wedge (j \not\simeq 0) \wedge (j \leq (p \div 2)))$
$\rightarrow \quad (\text{w}\,(j * q, \text{mults}\,(q \div 2,\, p)) = ((j * q) \div p))$

THEOREM: equal-wins-sum-quotients
$(\text{prime}\,(p) \wedge (\neg\, \text{divides}\,(p,\, q)) \wedge (j \leq (p \div 2)))$
$\rightarrow \quad (\text{sum}\,(\text{quotients}\,(j,\, q,\, p)) = \text{wins}\,(\text{mults}\,(j,\, q), \text{mults}\,(q \div 2,\, p)))$

THEOREM: law-of-quadratic-reciprocity
$(\text{prime}\,(p) \wedge (p \neq 2) \wedge \text{prime}\,(q) \wedge (q \neq 2) \wedge (p \neq q))$
$\rightarrow \quad ((\text{residue}\,(q,\, p) = \text{residue}\,(p,\, q)) = \text{even}\,((p \div 2) * (q \div 2)))$

Index