#|
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.

|#

; Work of David Russinoff.

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

EVENT: For efficiency, compile those definitions not yet compiled.

DEFINITION:
inverse $(j,\ p)$
$=$ **if** $p = 2$ **then** j **mod** 2
else $\exp(j,\ p-2)$ **mod** p **endif**

THEOREM: inverse-inverts-lemma
$(p \not\simeq 0) \rightarrow (((\text{inverse}(j,\ p) * j)\ \textbf{mod}\ p) = (\exp(j,\ p-1)\ \textbf{mod}\ p))$

THEOREM: inverse-inverts
$(\text{prime}(p) \wedge ((j\ \textbf{mod}\ p) \neq 0)) \rightarrow (((\text{inverse}(j,\ p) * j)\ \textbf{mod}\ p) = 1)$

THEOREM: inverse-is-unique
$(\text{prime}\,(p) \wedge (1 = ((m * x)\ \mathbf{mod}\ p))) \rightarrow (\text{inverse}\,(m,\ p) = (x\ \mathbf{mod}\ p))$

THEOREM: s-p-i-i-lemma1
$((n \not\simeq 0) \wedge (n \neq 1))$
$\rightarrow \quad (((n - 1) * (n - 1)) = (1 + (n * ((n - 1) - 1))))$

THEOREM: s-p-i-i-lemma2
$((n \not\simeq 0) \wedge (n \neq 1)) \rightarrow ((((n - 1) * (n - 1))\ \mathbf{mod}\ n) = 1)$

THEOREM: sub1-p-is-involution
$\text{prime}\,(p) \rightarrow (\text{inverse}\,(p - 1,\ p) = (p - 1))$

THEOREM: n-o-i-lemma1
$((x * x) - 1) = ((1 + x) * (x - 1))$

THEOREM: n-o-i-lemma2
$(\text{prime}\,(p) \wedge ((((j * j) - 1)\ \mathbf{mod}\ p) = 0))$
$\rightarrow \quad ((((1 + j)\ \mathbf{mod}\ p) = 0) \vee (((j - 1)\ \mathbf{mod}\ p) = 0))$

THEOREM: n-o-i-lemma3
$((a \not< 1) \wedge ((a\ \mathbf{mod}\ p) = 1)) \rightarrow (((a - 1)\ \mathbf{mod}\ p) = 0)$

THEOREM: n-o-i-lemma4
$(\text{prime}\,(p) \wedge ((j\ \mathbf{mod}\ p) \neq 0) \wedge (\text{inverse}\,(j,\ p) = j))$
$\rightarrow \quad ((((1 + j)\ \mathbf{mod}\ p) = 0) \vee (((j - 1)\ \mathbf{mod}\ p) = 0))$

THEOREM: no-other-involutions
$(\text{prime}\,(p) \wedge (j < (p - 1)) \wedge (1 < j)) \rightarrow (\text{inverse}\,(j,\ p) \neq j)$

THEOREM: i-o-i-lemma
$(((p - 2) * (p - 2)) - 1) = ((p - 3) * (p - 1))$

THEOREM: inverse-of-inverse
$(\text{prime}\,(p) \wedge ((j\ \mathbf{mod}\ p) \neq 0))$
$\rightarrow \quad (\text{inverse}\,(\text{inverse}\,(j,\ p),\ p) = (j\ \mathbf{mod}\ p))$

THEOREM: n-z-i-lemma
$((i \simeq 0) \wedge (1 < p)) \rightarrow (\text{inverse}\,(i,\ p) = 0)$

THEOREM: non-zerop-inverse
$(\text{prime}\,(p) \wedge ((j\ \mathbf{mod}\ p) \neq 0)) \rightarrow (\text{inverse}\,(j,\ p) \not\simeq 0)$

THEOREM: b-i-lemma2
$(\text{prime}\,(p) \wedge ((j\ \mathbf{mod}\ p) \neq 0) \wedge (\text{inverse}\,(j,\ p) = (p - 1)))$
$\rightarrow \quad ((j\ \mathbf{mod}\ p) = (p - 1))$

THEOREM: b-i-lemma1
$(1 < p) \rightarrow (\text{inverse}(j, p) \leq (p - 1))$

THEOREM: bounded-inverse
$(\text{prime}(p) \wedge (j < (p - 1))) \rightarrow (\text{inverse}(j, p) < (p - 1))$

DEFINITION:
inverse-list (i, p)
$=$ **if** $i \simeq 0$ **then nil**
elseif $i = 1$ **then** cons $(1,$ **nil**$)$
elseif $i \in$ inverse-list $(i - 1, p)$ **then** inverse-list $(i - 1, p)$
else cons $(i,$ cons $(\text{inverse}(i, p),$ inverse-list $(i - 1, p)))$ **endif**

THEOREM: all-non-zerop-inverse-list
$(\text{prime}(p) \wedge (i < (p - 1))) \rightarrow$ all-non-zerop (inverse-list (i, p))

THEOREM: bounded-inverse-list
$(\text{prime}(p) \wedge (i < (p - 1)) \wedge (j = (p - 2)))$
$\rightarrow$ all-lesseqp (inverse-list $(i, p), j$)

THEOREM: subsetp-positives
subsetp (positives (n), inverse-list (n, p))

THEOREM: inverse-1
$(1 < p) \rightarrow (\text{inverse}(1, p) = 1)$

THEOREM: a-d-i-l-lemma1
$(\text{prime}(p) \wedge ((i \textbf{ mod } p) \neq 0) \wedge (i < p) \wedge (j \in$ inverse-list $(i, p)))$
$\rightarrow$ $(\text{inverse}(j, p) \in$ inverse-list $(i, p))$

THEOREM: a-d-i-l-lemma2
$(\text{prime}(p)$
$\wedge$ $((i \textbf{ mod } p) \neq 0)$
$\wedge$ $((j \textbf{ mod } p) \neq 0)$
$\wedge$ $(i < p)$
$\wedge$ $(j < p)$
$\wedge$ $(\text{inverse}(j, p) \in$ inverse-list $(i, p)))$
$\rightarrow$ $(j \in$ inverse-list $(i, p))$

THEOREM: a-d-i-l-lemma3
$(\text{prime}(p) \wedge (i < (p - 1)) \wedge$ all-distinct (inverse-list $(i - 1, p)))$
$\rightarrow$ all-distinct (inverse-list (i, p))

THEOREM: all-distinct-inverse-list
$(\text{prime}(p) \wedge (i < (p - 1))) \rightarrow$ all-distinct (inverse-list (i, p))

THEOREM: t-i-l-lemma1
$(((a * b)\ \mathbf{mod}\ p) = 1) \rightarrow (((a * (b * c))\ \mathbf{mod}\ p) = (c\ \mathbf{mod}\ p))$

THEOREM: t-i-l-lemma
$(((i * \text{inverse}\,(i,\ p))\ \mathbf{mod}\ p) = 1)$
$\rightarrow\ ((\text{times-list}\,(\text{inverse-list}\,(i,\ p))\ \mathbf{mod}\ p)$
$=\ (\text{times-list}\,(\text{inverse-list}\,(i - 1,\ p))\ \mathbf{mod}\ p))$

THEOREM: t-i-l-lemma3
$(\text{prime}\,(p) \wedge ((i\ \mathbf{mod}\ p) \neq 0))$
$\rightarrow\ ((\text{times-list}\,(\text{inverse-list}\,(i,\ p))\ \mathbf{mod}\ p)$
$=\ (\text{times-list}\,(\text{inverse-list}\,(i - 1,\ p))\ \mathbf{mod}\ p))$

THEOREM: t-i-l-lemma4
$(i \leq 1) \rightarrow (\text{times-list}\,(\text{inverse-list}\,(i,\ p)) = 1)$

THEOREM: times-inverse-list
$(\text{prime}\,(p) \wedge (i < p)) \rightarrow ((\text{times-list}\,(\text{inverse-list}\,(i,\ p))\ \mathbf{mod}\ p) = 1)$

THEOREM: delete-x-leave-a
$((a \in s) \wedge (a \neq x)) \rightarrow (a \in \text{delete}\,(x,\ s))$

THEOREM: delete-member-leave-subset
$(\text{subsetp}\,(r,\ s) \wedge (x \notin r)) \rightarrow \text{subsetp}\,(r,\ \text{delete}\,(x,\ s))$

THEOREM: all-lesseqp-delete
$(\text{all-distinct}\,(l) \wedge \text{all-lesseqp}\,(l,\ n)) \rightarrow \text{all-lesseqp}\,(\text{delete}\,(n,\ l),\ n - 1)$

THEOREM: positives-bounded
$(n < m) \rightarrow (m \notin \text{positives}\,(n))$

THEOREM: subsetp-positives-delete
$\text{subsetp}\,(\text{positives}\,(n),\ l) \rightarrow \text{subsetp}\,(\text{positives}\,(n - 1),\ \text{delete}\,(n,\ l))$

THEOREM: nonzerop-lesseqp-zero
$((n \simeq 0) \wedge \text{all-lesseqp}\,(l,\ n) \wedge \text{all-non-zerop}\,(l)) \rightarrow (\neg\ \text{listp}\,(l))$

DEFINITION:
pigeonhole2-induction$\,(l,\ n)$
$=$ **if** $n \simeq 0$ **then t**
else pigeonhole2-induction$\,(\text{delete}\,(n,\ l),\ n - 1)$ **endif**

THEOREM: pigeonhole2
$(\text{all-distinct}\,(l)$
$\wedge\ \text{all-non-zerop}\,(l)$
$\wedge\ \text{all-lesseqp}\,(l,\ n)$
$\wedge\ \text{subsetp}\,(\text{positives}\,(n),\ l))$
$\rightarrow\ \text{perm}\,(\text{positives}\,(n),\ l)$

THEOREM: perm-positives-inverse-list
$(\text{prime}\,(p) \wedge (i = (p - 2))) \rightarrow \text{perm}\,(\text{positives}\,(i),\ \text{inverse-list}\,(i,\ p))$

THEOREM: inverse-list-fact
$(\text{prime}\,(p) \wedge (i = (p - 2)))$
$\rightarrow \quad (\text{times-list}\,(\text{inverse-list}\,(i,\ p)) = \text{fact}\,(i))$

THEOREM: w-t-lemma
$(\text{prime}\,(p) \wedge (i = (p - 2))) \rightarrow ((\text{fact}\,(i)\ \textbf{mod}\ p) = 1)$

THEOREM: wilson-thm
$\text{prime}\,(p) \rightarrow ((\text{fact}\,(p - 1)\ \textbf{mod}\ p) = (p - 1))$

EVENT: Make the library `"wilson"` and compile it.

Index

a-d-i-l-lemma1, 3
a-d-i-l-lemma2, 3
a-d-i-l-lemma3, 3
all-distinct, 3, 4
all-distinct-inverse-list, 3
all-lesseqp, 3, 4
all-lesseqp-delete, 4
all-non-zerop, 3, 4
all-non-zerop-inverse-list, 3

b-i-lemma1, 3
b-i-lemma2, 2
bounded-inverse, 3
bounded-inverse-list, 3

delete, 4
delete-member-leave-subset, 4
delete-x-leave-a, 4

exp, 1

fact, 5

i-o-i-lemma, 2
inverse, 1–4
inverse-1, 3
inverse-inverts, 1
inverse-inverts-lemma, 1
inverse-is-unique, 2
inverse-list, 3–5
inverse-list-fact, 5
inverse-of-inverse, 2

n-o-i-lemma1, 2
n-o-i-lemma2, 2
n-o-i-lemma3, 2
n-o-i-lemma4, 2
n-z-i-lemma, 2
no-other-involutions, 2
non-zerop-inverse, 2
nonzerop-lesseqp-zero, 4

perm, 4, 5
perm-positives-inverse-list, 5
pigeonhole2, 4
pigeonhole2-induction, 4
positives, 3–5
positives-bounded, 4
prime, 1–5

s-p-i-i-lemma1, 2
s-p-i-i-lemma2, 2
sub1-p-is-involution, 2
subsetp, 3, 4
subsetp-positives, 3
subsetp-positives-delete, 4

t-i-l-lemma, 4
t-i-l-lemma1, 4
t-i-l-lemma3, 4
t-i-l-lemma4, 4
times-inverse-list, 4
times-list, 4, 5

w-t-lemma, 5
wilson-thm, 5