```
; 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
$(p \not\simeq 0) \rightarrow (((\text{inverse}(j,\ p) * j) \ \mathbf{mod}\ p) = (\exp(j,\ p - 1)\ \mathbf{mod}\ p))$

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

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

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

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

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

THEOREM: n-o-i-lemma1
$((x * x) - \mathtt{1}) = ((1 + x) * (x - 1))$

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

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

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

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

THEOREM: i-o-i-lemma
$(((p - \mathtt{2}) * (p - \mathtt{2})) - 1) = ((p - \mathtt{3}) * (p - 1))$

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

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

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

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

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:
$$
\begin{aligned}
&\text{inverse-list}\,(i,\ p)\\
= \quad & \textbf{if } i \simeq 0 \textbf{ then nil}\\
& \textbf{elseif } i = 1 \textbf{ then } \text{cons}\,(1,\ \textbf{nil})\\
& \textbf{elseif } i \in \text{inverse-list}\,(i - 1,\ p) \textbf{ then } \text{inverse-list}\,(i - 1,\ p)\\
& \textbf{else } \text{cons}\,(i,\ \text{cons}\,(\text{inverse}\,(i,\ p),\ \text{inverse-list}\,(i - 1,\ p))) \textbf{ endif}
\end{aligned}
$$

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

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

THEOREM: subsetp-positives
$\text{subsetp}\,(\text{positives}\,(n),\ \text{inverse-list}\,(n,\ p))$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Index