```
; Work of David Russinoff.
```

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

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

DEFINITION:
squares (n, p)
$= \;$ **if** $n \simeq 0$ **then** list (0)
else cons $((n * n)$ **mod** p, squares $(n - 1, p))$ **endif**

DEFINITION:
residue $(a, p) = ((\neg \text{ divides}(p, a)) \wedge ((a \textbf{ mod } p) \in \text{squares}(p, p)))$

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

THEOREM: all-squares-2
$((y * y) \textbf{ mod } p) = (((y \textbf{ mod } p) * (y \textbf{ mod } p)) \textbf{ mod } p)$

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

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

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

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

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

THEOREM: euler-1-5
$(\text{prime}(p) \land (\neg \text{divides}(p, a)) \land ((a \textbf{ mod } p) = ((i * i) \textbf{ mod } p)))$
$\rightarrow \quad (\neg \text{divides}(p, i))$

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

THEOREM: euler-1-7
$(\text{prime}(p)$
$\land \quad (\neg \text{divides}(2, p))$
$\land \quad (\neg \text{divides}(p, a))$
$\land \quad ((a \textbf{ mod } p) \in \text{squares}(i, p)))$
$\rightarrow \quad ((\exp(a, p \div 2) \textbf{ mod } p) = 1)$

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

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

EVENT: Enable inverse; name this event ‘g0219’.

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

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

EVENT: Enable complement; name this event 'complement-off'.

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

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

EVENT: Enable squares; name this event 'squares-off'.

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

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

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

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

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

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

THEOREM: comp-list-closed-1
$$
\begin{array}{ll}
\multicolumn{2}{l}{(\text{prime}\,(p)} \\
\wedge & (i \not\simeq \mathsf{0}) \\
\wedge & (i < p) \\
\wedge & (\neg\ \text{divides}\,(p,\ a)) \\
\wedge & (j \in \text{comp-list}\,(i,\ a,\ p))) \\
\rightarrow & (\text{complement}\,(j,\ a,\ p) \in \text{comp-list}\,(i,\ a,\ p))
\end{array}
$$

THEOREM: comp-list-closed-2
$$
\begin{array}{ll}
\multicolumn{2}{l}{(\text{prime}\,(p)} \\
\wedge & (i \not\simeq \mathsf{0}) \\
\wedge & (j \not\simeq \mathsf{0}) \\
\wedge & (i < p) \\
\wedge & (j < p) \\
\wedge & (\neg\ \text{divides}\,(p,\ a)) \\
\wedge & (\text{complement}\,(j,\ a,\ p) \in \text{comp-list}\,(i,\ a,\ p))) \\
\rightarrow & (j \in \text{comp-list}\,(i,\ a,\ p))
\end{array}
$$

THEOREM: all-distinct-comp-list-1
$$
\begin{array}{ll}
\multicolumn{2}{l}{(\text{prime}\,(p)} \\
\wedge & (i < p) \\
\wedge & (\neg\ \text{divides}\,(p,\ a)) \\
\wedge & (\neg\ \text{residue}\,(a,\ p)) \\
\wedge & \text{all-distinct}\,(\text{comp-list}\,(i - 1,\ a,\ p))) \\
\rightarrow & \text{all-distinct}\,(\text{comp-list}\,(i,\ a,\ p))
\end{array}
$$

THEOREM: all-distinct-comp-list
$$
\begin{array}{ll}
\multicolumn{2}{l}{(\text{prime}\,(p) \wedge (i < p) \wedge (\neg\ \text{divides}\,(p,\ a)) \wedge (\neg\ \text{residue}\,(a,\ p)))} \\
\rightarrow & \text{all-distinct}\,(\text{comp-list}\,(i,\ a,\ p))
\end{array}
$$

THEOREM: perm-positives-comp-list
$$
\begin{array}{ll}
\multicolumn{2}{l}{(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ a)) \wedge (\neg\ \text{residue}\,(a,\ p)))} \\
\rightarrow & \text{perm}\,(\text{positives}\,(p - 1),\ \text{comp-list}\,(p - 1,\ a,\ p))
\end{array}
$$

THEOREM: comp-list-fact
$$
\begin{array}{ll}
\multicolumn{2}{l}{(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ a)) \wedge (\neg\ \text{residue}\,(a,\ p)))} \\
\rightarrow & (\text{times-list}\,(\text{comp-list}\,(p - 1,\ a,\ p)) = \text{fact}\,(p - 1))
\end{array}
$$

THEOREM: times-mod-4
$$
\begin{array}{ll}
\multicolumn{2}{l}{(((i * j)\ \mathbf{mod}\ p) = (a\ \mathbf{mod}\ p))} \\
\rightarrow & (((i * (j * k))\ \mathbf{mod}\ p) = ((a * (k\ \mathbf{mod}\ p))\ \mathbf{mod}\ p))
\end{array}
$$

THEOREM: times-comp-list-1
$$
\begin{array}{ll}
\multicolumn{2}{l}{((((i * \text{complement}\,(i,\ a,\ p))\ \mathbf{mod}\ p) = (a\ \mathbf{mod}\ p))} \\
\wedge & (i \not\simeq \mathsf{0})
\end{array}
$$

$\wedge \quad (i \not\in \text{comp-list}\,(i - 1,\ a,\ p)))$
$\rightarrow \quad ((\text{times-list}\,(\text{comp-list}\,(i,\ a,\ p))\ \textbf{mod}\ p)$
$\quad\quad = \quad ((a * (\text{times-list}\,(\text{comp-list}\,(i - 1,\ a,\ p))\ \textbf{mod}\ p))\ \textbf{mod}\ p))$

THEOREM: times-comp-list-2
$(\text{prime}\,(p) \wedge (\neg\ \text{divides}\,(p,\ i)) \wedge (i \not\in \text{comp-list}\,(i - 1,\ a,\ p)))$
$\rightarrow \quad ((\text{times-list}\,(\text{comp-list}\,(i,\ a,\ p))\ \textbf{mod}\ p)$
$\quad\quad = \quad ((a * (\text{times-list}\,(\text{comp-list}\,(i - 1,\ a,\ p))\ \textbf{mod}\ p))\ \textbf{mod}\ p))$

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

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

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

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

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

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
$(\text{prime}(p) \wedge (\neg \text{divides}(p, a)) \wedge (\neg \text{residue}(a, p)))$
$\rightarrow \quad ((\exp(a, \text{length}(\text{comp-list}(p - 1, a, p)) \div 2) \textbf{ mod } p) = (p - 1))$

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

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

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

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

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

DEFINITION: $\text{reflect}(x, p) = (p - x)$

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

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
$((x < p) \wedge (x \not\simeq 0) \wedge (b \not\simeq 0))$
$\rightarrow \quad ((((b * p) - x) \textbf{ mod } p) = (p - x))$

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

Theorem: reflect-commutes-with-times-2
$(y \le p)$
$\rightarrow \quad (((x * \text{reflect}\,(y,\ p))\ \mathbf{mod}\ p) = (\text{reflect}\,((x * y)\ \mathbf{mod}\ p,\ p)\ \mathbf{mod}\ p))$

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

Theorem: rem-reflect-list-1
$((p \not\simeq \mathsf{0})$
$\ \wedge \quad (n \not\simeq \mathsf{0})$
$\ \wedge \quad ((p \div \mathsf{2}) \not< ((a * n)\ \mathbf{mod}\ p))$
$\ \wedge \quad ((\text{times-list}\,(\text{reflect-list}\,(n-1,\ a,\ p))\ \mathbf{mod}\ p)$
$\qquad = \quad ((\exp\,(a,\ n-1) * \text{fact}\,(n-1))\ \mathbf{mod}\ p)))$
$\rightarrow \quad ((\text{times-list}\,(\text{reflect-list}\,(n,\ a,\ p))\ \mathbf{mod}\ p)$
$\qquad = \quad ((\exp\,(a,\ n) * \text{fact}\,(n))\ \mathbf{mod}\ p))$

Theorem: rem-reflect-list-2
$((p \not\simeq \mathsf{0})$
$\ \wedge \quad (n \not\simeq \mathsf{0})$
$\ \wedge \quad ((p \div \mathsf{2}) < ((a * n)\ \mathbf{mod}\ p))$
$\ \wedge \quad ((\text{times-list}\,(\text{reflect-list}\,(n-1,\ a,\ p))\ \mathbf{mod}\ p)$
$\qquad = \quad ((\exp\,(a,\ n-1) * \text{fact}\,(n-1))\ \mathbf{mod}\ p)))$
$\rightarrow \quad ((\text{times-list}\,(\text{reflect-list}\,(n,\ a,\ p))\ \mathbf{mod}\ p)$
$\qquad = \quad (\text{reflect}\,((\exp\,(a,\ n) * \text{fact}\,(n))\ \mathbf{mod}\ p,\ p)\ \mathbf{mod}\ p))$

Theorem: rem-reflect-list-3
$((p \not\simeq \mathsf{0})$
$\ \wedge \quad (n \not\simeq \mathsf{0})$
$\ \wedge \quad ((p \div \mathsf{2}) \not< ((a * n)\ \mathbf{mod}\ p))$
$\ \wedge \quad ((\text{times-list}\,(\text{reflect-list}\,(n-1,\ a,\ p))\ \mathbf{mod}\ p)$
$\qquad = \quad (\text{reflect}\,((\exp\,(a,\ n-1) * \text{fact}\,(n-1))\ \mathbf{mod}\ p,\ p)\ \mathbf{mod}\ p)))$
$\rightarrow \quad ((\text{times-list}\,(\text{reflect-list}\,(n,\ a,\ p))\ \mathbf{mod}\ p)$
$\qquad = \quad (\text{reflect}\,((\exp\,(a,\ n) * \text{fact}\,(n))\ \mathbf{mod}\ p,\ p)\ \mathbf{mod}\ p))$

Theorem: double-reflect
$(a \le p) \rightarrow ((\text{reflect}\,(\text{reflect}\,(a,\ p)\ \mathbf{mod}\ p,\ p)\ \mathbf{mod}\ p) = (a\ \mathbf{mod}\ p))$

Theorem: rem-reflect-list-4
$((p \not\simeq \mathsf{0})$
$\ \wedge \quad (n \not\simeq \mathsf{0})$
$\ \wedge \quad ((p \div \mathsf{2}) < ((a * n)\ \mathbf{mod}\ p))$
$\ \wedge \quad ((\text{times-list}\,(\text{reflect-list}\,(n-1,\ a,\ p))\ \mathbf{mod}\ p)$
$\qquad = \quad (\text{reflect}\,((\exp\,(a,\ n-1) * \text{fact}\,(n-1))\ \mathbf{mod}\ p,\ p)\ \mathbf{mod}\ p)))$
$\rightarrow \quad ((\text{times-list}\,(\text{reflect-list}\,(n,\ a,\ p))\ \mathbf{mod}\ p)$
$\qquad = \quad ((\exp\,(a,\ n) * \text{fact}\,(n))\ \mathbf{mod}\ p))$

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

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

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

THEOREM: all-lesseqp-reflect-list-1
$((p \div 2) < x) \rightarrow ((p \div 2) \not< \text{reflect}\,(x,\ p))$

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

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

THEOREM: all-distinct-reflect-list-1
$(\text{prime}\,(p) \land (j < i) \land (i < p) \land (\neg\ \text{divides}\,(p,\ a)))$
$\rightarrow \quad (((a * i)\ \mathbf{mod}\ p) \neq ((a * j)\ \mathbf{mod}\ p))$

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

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

THEOREM: all-distinct-reflect-list-3
$(\text{prime}\,(p) \land (j < i) \land (i < p) \land (\neg\ \text{divides}\,(p,\ a)))$
$\rightarrow \quad (\text{reflect}\,((a * i)\ \mathbf{mod}\ p,\ p) \neq \text{reflect}\,((a * j)\ \mathbf{mod}\ p,\ p))$

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

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

THEOREM: all-distinct-reflect-list-4
$((x = (p - y)) \land (y < p)) \rightarrow (((x + y)\ \mathbf{mod}\ p) = 0)$

THEOREM: all-distinct-reflect-list-5
$((((a * i) \ \mathbf{mod}\ p) = (p - ((a * j) \ \mathbf{mod}\ p))) \wedge (p \not\simeq 0))$
$\rightarrow \quad (((a * (i + j)) \ \mathbf{mod}\ p) = 0)$

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

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

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

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

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

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

THEOREM: times-reflect-list
$(\text{prime}(p) \wedge (\neg \text{divides}(2, p)) \wedge (\neg \text{divides}(p, a)))$
$\rightarrow \quad (\text{times-list}(\text{reflect-list}(p \div 2, a, p)) = \text{fact}(p \div 2))$

THEOREM: plus-x-x-even
$((x + x) \ \mathbf{mod}\ 2) = 0$

THEOREM: res1-rem-1-1
$((x \not\simeq 0) \wedge (\neg \operatorname{divides}(2,\ p))) \rightarrow (((p - x) \mathbf{\ mod\ } p) \neq x)$

THEOREM: res1-rem-1
$(\operatorname{prime}(p)$
$\wedge \quad (\neg \operatorname{divides}(2,\ p))$
$\wedge \quad (\neg \operatorname{divides}(p,\ a))$
$\wedge \quad \operatorname{res1}(p \div 2,\ a,\ p))$
$\rightarrow \quad ((\exp(a,\ p \div 2) \mathbf{\ mod\ } p) = 1)$

THEOREM: remainder-lessp
$(a < p) \rightarrow ((a \mathbf{\ mod\ } p) = \operatorname{fix}(a))$

THEOREM: res1-rem-2
$(\operatorname{prime}(p)$
$\wedge \quad (\neg \operatorname{divides}(2,\ p))$
$\wedge \quad (\neg \operatorname{divides}(p,\ a))$
$\wedge \quad (\neg \operatorname{res1}(p \div 2,\ a,\ p)))$
$\rightarrow \quad ((\exp(a,\ p \div 2) \mathbf{\ mod\ } p) \neq 1)$

THEOREM: two-even
$(\neg \operatorname{divides}(2,\ p)) \rightarrow ((p - 1) \neq 1)$

THEOREM: gauss-lemma
$(\operatorname{prime}(p) \wedge (\neg \operatorname{divides}(p,\ a)) \wedge (\neg \operatorname{divides}(2,\ p)))$
$\rightarrow \quad (\operatorname{res1}(p \div 2,\ a,\ p) = \operatorname{residue}(a,\ p))$

DEFINITION:
$\text{plus-list}(l)$
$= \quad \mathbf{if}\ l \simeq \mathbf{nil}\ \ \mathbf{then}\ 0$
$\quad\quad \mathbf{else}\ \operatorname{car}(l) + \text{plus-list}(\operatorname{cdr}(l))\ \mathbf{endif}$

DEFINITION:
$\text{quot-list}(n,\ a,\ p)$
$= \quad \mathbf{if}\ n \simeq 0\ \ \mathbf{then}\ \mathbf{nil}$
$\quad\quad \mathbf{else}\ \operatorname{cons}((a * n) \div p,\ \text{quot-list}(n - 1,\ a,\ p))\ \mathbf{endif}$

DEFINITION:
$\text{rem-list}(n,\ a,\ p)$
$= \quad \mathbf{if}\ n \simeq 0\ \ \mathbf{then}\ \mathbf{nil}$
$\quad\quad \mathbf{else}\ \operatorname{cons}((a * n) \mathbf{\ mod\ } p,\ \text{rem-list}(n - 1,\ a,\ p))\ \mathbf{endif}$

THEOREM: rem-quot-list
$(a * \text{plus-list}(\operatorname{positives}(n)))$
$= \quad ((p * \text{plus-list}(\text{quot-list}(n,\ a,\ p))) + \text{plus-list}(\text{rem-list}(n,\ a,\ p)))$

DEFINITION:
$\text{even3}(x)$
$= \ \ \textbf{if } x \simeq 0 \textbf{ then t}$
$\quad \textbf{else} \neg \text{even3}(x - 1) \textbf{ endif}$

THEOREM: even3-plus
$\text{even3}(a + b) = (\text{even3}(a) = \text{even3}(b))$

THEOREM: even3-diff
$(x \leq p) \rightarrow (\text{even3}(p - x) = (\text{even3}(p) = \text{even3}(x)))$

THEOREM: even3-times
$\text{even3}(a * b) = (\text{even3}(a) \vee \text{even3}(b))$

THEOREM: even3-rem
$(\neg \text{even3}(p)) \rightarrow (\text{even3}(p - (x \textbf{ mod } p)) = (\neg \text{even3}(x \textbf{ mod } p)))$

THEOREM: even3-rem-reflect
$(\neg \text{even3}(p))$
$\rightarrow \ \ (\text{res1}(n, a, p)$
$\quad = \ \ (\text{even3}(\text{plus-list}(\text{rem-list}(n, a, p)))$
$\quad\quad \leftrightarrow \ \ \text{even3}(\text{plus-list}(\text{reflect-list}(n, a, p)))))$

THEOREM: perm-plus-list-1
$(x \in m) \rightarrow ((x + \text{plus-list}(\text{delete}(x, m))) = \text{plus-list}(m))$

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

THEOREM: even3-even
$\text{divides}(2, p) = \text{even3}(p)$

THEOREM: plus-reflect-list
$(\text{prime}(p) \wedge (\neg \text{divides}(p, a)) \wedge (\neg \text{even3}(p)))$
$\rightarrow \ \ (\text{plus-list}(\text{reflect-list}(p \div 2, a, p))$
$\quad = \ \ \text{plus-list}(\text{positives}(p \div 2)))$

THEOREM: equals-have-same-parity
$(x = y) \rightarrow (\text{even3}(x) = \text{even3}(y))$

THEOREM: res1-quot-list
$(\text{prime}(p) \wedge (\neg \text{even3}(p)) \wedge (\neg \text{even3}(a)) \wedge (\neg \text{divides}(p, a)))$
$\rightarrow \ \ (\text{res1}(p \div 2, a, p) = \text{even3}(\text{plus-list}(\text{quot-list}(p \div 2, a, p))))$

DEFINITION:
$\text{wins1}(x, l)$
$= \ \ \textbf{if } l \simeq \textbf{nil then } 0$
$\quad \textbf{elseif } \text{car}(l) < x \textbf{ then } 1 + \text{wins1}(x, \text{cdr}(l))$
$\quad \textbf{else } \text{wins1}(x, \text{cdr}(l)) \textbf{ endif}$

DEFINITION:
wins $(k,\ l)$
$=$ **if** $k \simeq$ **nil** **then** 0
else wins1 $(\text{car}(k),\ l) +$ wins $(\text{cdr}(k),\ l)$ **endif**

DEFINITION:
losses1 $(x,\ l)$
$=$ **if** $l \simeq$ **nil** **then** 0
elseif $x < \text{car}(l)$ **then** $1 +$ losses1 $(x,\ \text{cdr}(l))$
else losses1 $(x,\ \text{cdr}(l))$ **endif**

DEFINITION:
losses $(k,\ l)$
$=$ **if** $k \simeq$ **nil** **then** 0
else losses1 $(\text{car}(k),\ l) +$ losses $(\text{cdr}(k),\ l)$ **endif**

THEOREM: win-some-lose-some-1
$((x \notin l) \land \text{all-non-zerop}(l))$
$\rightarrow \quad ((\text{losses1}(x,\ l) + \text{wins1}(x,\ l)) = \text{length}(l))$

THEOREM: win-some-lose-some-2
$((\text{intersect}(l,\ m) \simeq \textbf{nil}) \land \text{all-non-zerop}(l) \land \text{all-non-zerop}(m))$
$\rightarrow \quad ((\text{wins}(l,\ m) + \text{losses}(l,\ m)) = (\text{length}(l) * \text{length}(m)))$

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

THEOREM: a-winner-every-time
$((\text{intersect}(l,\ m) \simeq \textbf{nil}) \land \text{all-non-zerop}(l) \land \text{all-non-zerop}(m))$
$\rightarrow \quad ((\text{wins}(l,\ m) + \text{wins}(m,\ l)) = (\text{length}(l) * \text{length}(m)))$

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

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

THEOREM: leq-n-wins1
$((n * p) < a) \rightarrow (n \leq \text{wins1}(a,\ \text{mults}(n,\ p)))$

THEOREM: monotone-wins1
$(n \leq m) \rightarrow (\text{wins1}(a,\ \text{mults}(n,\ p)) \leq \text{wins1}(a,\ \text{mults}(m,\ p)))$

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

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

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

DEFINITION:
monotone-quot-induction $(i,\ j,\ p)$
$=$ **if** $p \simeq 0$ **then t**
elseif $i < p$ **then t**
elseif $j < p$ **then t**
else monotone-quot-induction $(i - p,\ j - p,\ p)$ **endif**

THEOREM: monotone-quot
$(j \leq i) \rightarrow ((j \div p) \leq (i \div p))$

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

THEOREM: leq-quot-wins1-1
$(\neg\ \text{divides}\,(p,\ x)) \rightarrow (((x \div p) * p) < x)$

THEOREM: leq-quot-wins1-2
$(\text{prime}\,(p) \land (\neg\ \text{divides}\,(p,\ q)) \land (q \not\simeq 0) \land (j \not\simeq 0) \land (j < p))$
$\rightarrow\quad ((((j * q) \div p) * p) < (j * q))$

THEOREM: leq-quot-wins1
$(\text{prime}\,(p)$
$\land\quad (\neg\ \text{divides}\,(p,\ q))$
$\land\quad (j \leq (p \div 2))$
$\land\quad (j \not\simeq 0)$
$\land\quad (q \not\simeq 0))$
$\rightarrow\quad (((j * q) \div p) \leq \text{wins1}\,(j * q,\ \text{mults}\,(q \div 2,\ p)))$

DEFINITION:
wins2 $(a,\ n,\ p)$
$=$ **if** $n \simeq 0$ **then** 0
elseif $(n * p) < a$ **then** n
else wins2 $(a,\ n - 1,\ p)$ **endif**

Theorem: leq-wins2
$(\text{wins2}(a,\ n,\ p) * p) \le a$

Theorem: leq-wins1-n
$\text{wins1}(a,\ \text{mults}(n,\ p)) \le n$

Theorem: leq-wins1-wins2
$\text{wins1}(a,\ \text{mults}(n,\ p)) \le \text{wins2}(a,\ n,\ p)$

Theorem: leq-wins1
$(\text{wins1}(a,\ \text{mults}(n,\ p)) * p) \le a$

Theorem: leq-wins1-quot
$(p \not\simeq 0) \to (\text{wins1}(a,\ \text{mults}(n,\ p)) \le (a \div p))$

Theorem: equal-quot-wins1
$$
\begin{array}{ll}
(\text{prime}(p) & \\
\ \wedge & (\neg\ \text{divides}(p,\ q)) \\
\ \wedge & (j \le (p \div 2)) \\
\ \wedge & (j \not\simeq 0) \\
\ \wedge & (q \not\simeq 0)) \\
\to & (\text{wins1}(j * q,\ \text{mults}(q \div 2,\ p)) = ((j * q) \div p))
\end{array}
$$

Theorem: equal-wins-plus-quot-list
$$
\begin{array}{ll}
(\text{prime}(p) & \\
\ \wedge & (\neg\ \text{divides}(p,\ q)) \\
\ \wedge & (q \not\simeq 0) \\
\ \wedge & (j \not\simeq 0) \\
\ \wedge & (j \le (p \div 2))) \\
\to & (\text{wins}(\text{mults}(j,\ q),\ \text{mults}(q \div 2,\ p)) = \text{plus-list}(\text{quot-list}(j,\ q,\ p)))
\end{array}
$$

Theorem: gauss-corollary
$$
\begin{array}{ll}
\multicolumn{2}{l}{(\text{prime}(p) \wedge \text{prime}(q) \wedge (p \neq 2) \wedge (q \neq 2) \wedge (p \neq q))} \\
\to & (\text{res1}(p \div 2,\ q,\ p) = \text{residue}(q,\ p))
\end{array}
$$

Theorem: residue-quot-list
$$
\begin{array}{ll}
\multicolumn{2}{l}{(\text{prime}(p) \wedge \text{prime}(q) \wedge (p \neq q) \wedge (p \neq 2) \wedge (q \neq 2))} \\
\to & ((\text{residue}(q,\ p) = \text{residue}(p,\ q)) \\
 & \quad = \quad \text{even3}(\text{plus-list}(\text{quot-list}(p \div 2,\ q,\ p)) \\
 & \qquad\qquad\qquad + \quad \text{plus-list}(\text{quot-list}(q \div 2,\ p,\ q))))
\end{array}
$$

Theorem: all-non-zerop-mults
$(p \not\simeq 0) \to \text{all-non-zerop}(\text{mults}(n,\ p))$

Theorem: empty-intersect-mults-1
$$
\begin{array}{ll}
\multicolumn{2}{l}{(\text{prime}(p) \wedge \text{prime}(q) \wedge (p \neq q) \wedge (i < q) \wedge (j < p))} \\
\to & ((i * p) \notin \text{mults}(j,\ q))
\end{array}
$$

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

THEOREM: equal-plus-quot-list-wins
$(\text{prime}\,(p) \land \text{prime}\,(q) \land (p \neq q))$
$\rightarrow \quad (\text{plus-list}\,(\text{quot-list}\,(p \div 2,\ q,\ p))$
$\quad = \quad \text{wins}\,(\text{mults}\,(p \div 2,\ q),\ \text{mults}\,(q \div 2,\ p)))$

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

Index