```
; Matt Wilding
```


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

```
;; Proof of Matijasevich's lemma constructed by MW week of 5-10-91.  Inspired by
;; proof in Concrete Mathematics by Graham, Knuth, and Patashnik and notes from
;; Dijkstra's Capita Selecta Spring '90 course.

;;;; Some additional facts needed in the proof that appear useful
;;;; enough to add to libraries (and a few facts to prove them)
```

THEOREM: irem-igcd-arg1
$(\mathrm{irem}\,(\mathrm{igcd}\,(a,\ b),\ c) = 0) = ((\mathrm{irem}\,(a,\ c) = 0) \wedge (\mathrm{irem}\,(b,\ c) = 0))$

THEOREM: irem-x-x
$\mathrm{irem}\,(x,\ x) = 0$

```
;; The nonsensical induction hint is a silly trick to get the prover
;; to throw an equality away after using it
```

THEOREM: gcd-times-easy-proof-helper-helper
$((a \in \mathbf{N}) \land (b \in \mathbf{N}) \land (c \in \mathbf{N}))$
$\rightarrow \quad (((c * \mathrm{gcd}\,(a,\ b))\ \mathbf{mod}\ \mathrm{gcd}\,(a,\ b * c)) = \mathtt{0})$

THEOREM: gcd-times-easy-proof-helper
$((c * \mathrm{gcd}\,(a,\ b))\ \mathbf{mod}\ \mathrm{gcd}\,(a,\ b * c)) = \mathtt{0}$

THEOREM: gcd-times-easy-proof
$(\mathrm{gcd}\,(a,\ b) = \mathtt{1}) \rightarrow (\mathrm{gcd}\,(a,\ b * c) = \mathrm{gcd}\,(a,\ c))$

```
;; Would the more general case of rewriting gcd-times regardless
;; of the value of gcd with one of the times arguments be superior?
```

THEOREM: gcd-times-easy
$(\mathrm{gcd}\,(a,\ b) = \mathtt{1})$
$\rightarrow \quad ((\mathrm{gcd}\,(a,\ b * c) = \mathrm{gcd}\,(a,\ c)) \land (\mathrm{gcd}\,(a,\ c * b) = \mathrm{gcd}\,(a,\ c)))$

THEOREM: lessp-gcd3
$((\mathrm{gcd}\,(a,\ b) < a) = (((b\ \mathbf{mod}\ a) \neq \mathtt{0}) \land (a \not\simeq \mathtt{0}) \land (b \not\simeq \mathtt{0})))$
$\land \quad ((\mathrm{gcd}\,(b,\ a) < a) = (((b\ \mathbf{mod}\ a) \neq \mathtt{0}) \land (a \not\simeq \mathtt{0}) \land (b \not\simeq \mathtt{0})))$

THEOREM: equal-remainder-gcd-0-proof
$((\mathrm{gcd}\,(a,\ b)\ \mathbf{mod}\ a) = \mathtt{0}) = ((b\ \mathbf{mod}\ a) = \mathtt{0})$

```
;; not used in proof (though equal-remainder-gcd-0-proof is)
```

THEOREM: equal-remainder-gcd-0
$(((\mathrm{gcd}\,(a,\ b)\ \mathbf{mod}\ a) = \mathtt{0}) = ((b\ \mathbf{mod}\ a) = \mathtt{0}))$
$\land \quad (((\mathrm{gcd}\,(b,\ a)\ \mathbf{mod}\ a) = \mathtt{0}) = ((b\ \mathbf{mod}\ a) = \mathtt{0}))$

THEOREM: equal-remainder-x-y-x
$((x\ \mathbf{mod}\ y) = x)$
$= \quad (((x \in \mathbf{N}) \land (x < y))$
$\quad\quad \lor \quad (x = \mathtt{0})$
$\quad\quad \lor \quad ((\mathrm{fix}\,(y) = \mathtt{0}) \land (x \in \mathbf{N})))$

THEOREM: gcd-a-gcd-exp-a
$\mathrm{gcd}\,(a,\ \exp\,(a,\ b))$
$= \quad \mathbf{if}\ b \simeq \mathtt{0}\ \mathbf{then}\ \mathtt{1}$
$\quad\quad \mathbf{else}\ \mathrm{fix}\,(a)\ \mathbf{endif}$

THEOREM: equal-gcd-times-1-help1
$((\mathrm{gcd}\,(a,\ b) = \mathtt{1}) \land (\mathrm{gcd}\,(a,\ c) = \mathtt{1})) \rightarrow (\mathrm{gcd}\,(a,\ b * c) = \mathtt{1})$

THEOREM: remainder-gcd-gcd-0-hack
$(\mathrm{gcd}\,(a,\ b * c)\ \mathbf{mod}\ \mathrm{gcd}\,(a,\ c)) = \mathtt{0}$

THEOREM: lessp-gcd-times
$((a \not\simeq 0) \lor ((b * c) \not\simeq 0)) \rightarrow (\text{gcd}(a,\ b * c) \not< \text{gcd}(a,\ c))$

THEOREM: lessp-1-hack
$(1 < x) = ((x \not\simeq 0) \land (x \neq 1))$

THEOREM: equal-gcd-times-1-help2
$(\text{gcd}(a,\ b * c) = 1) \rightarrow (\text{gcd}(a,\ c) = 1)$

THEOREM: equal-gcd-times-1
$(\text{gcd}(a,\ b * c) = 1) = ((\text{gcd}(a,\ b) = 1) \land (\text{gcd}(a,\ c) = 1))$

THEOREM: gcd-exp-1
$((\text{gcd}(a, \exp(b,\ c)) = 1) = ((\text{gcd}(a,\ b) = 1) \lor (c \simeq 0)))$
$\land \quad ((\text{gcd}(\exp(b,\ c),\ a) = 1) = ((\text{gcd}(a,\ b) = 1) \lor (c \simeq 0)))$

```
;; mistake in other version of this lemma limits applicability and
;; makes this version needed
```

THEOREM: gcd-remainder-times-fact1-proof2
$(\text{gcd}(a,\ b) = 1) \rightarrow ((((c * b) \textbf{ mod } a) = 0) = ((c \textbf{ mod } a) = 0))$

THEOREM: times-quotient-better
$((x \textbf{ mod } y) = 0)$
$\rightarrow \quad ((((x \div y) * y)$
$\quad = \textbf{if } y \simeq 0 \textbf{ then } 0$
$\quad\quad \textbf{else } \text{fix}(x) \textbf{ endif})$
$\quad \land \quad ((y * (x \div y))$
$\quad\quad = \textbf{if } y \simeq 0 \textbf{ then } 0$
$\quad\quad\quad \textbf{else } \text{fix}(x) \textbf{ endif}))$

THEOREM: equal-remainder-exp-0
$(((a \textbf{ mod } c) = 0) \land (b \not\simeq 0)) \rightarrow ((\exp(a,\ b) \textbf{ mod } c) = 0)$

THEOREM: remainder-2-hack
$(2 \textbf{ mod } x)$
$= \textbf{if } (x = 1) \lor (x = 2) \textbf{ then } 0$
$\quad \textbf{else } 2 \textbf{ endif}$

THEOREM: remainder-times-hack2
$((a \textbf{ mod } b) \neq 0)$
$\rightarrow \quad (((a \textbf{ mod } (b * c)) \neq 0) \land ((a \textbf{ mod } (c * b)) \neq 0))$

THEOREM: gcd-a-add1-a
$\text{gcd}(a,\ 1 + a) = 1$

```
;; These facts should perhaps be generalized into a meta lemma that
;; factors first
```

THEOREM: remainder-times-times-hack
$((b * (a * c)) \ \mathbf{mod}\ (a * x)) = (a * ((b * c)\ \mathbf{mod}\ x))$

THEOREM: remainder-plus-times-hack
$(((a * x) + (b * (c * (a * y)))) \ \mathbf{mod}\ (a * z))$
$= \quad (a * ((x + (b * (c * y)))\ \mathbf{mod}\ z))$

```
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
;;; Now, on to the proof
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

DEFINITION:
$\mathrm{fib}(x)$
$= \quad \mathbf{if}\ x \simeq \mathtt{0}\ \ \mathbf{then}\ \mathtt{0}$
$\quad \mathbf{elseif}\ x = \mathtt{1}\ \ \mathbf{then}\ \mathtt{1}$
$\quad \mathbf{else}\ \mathrm{fib}((x - 1) - 1) + \mathrm{fib}(x - 1)\ \mathbf{endif}$

THEOREM: fib-plus
$\mathrm{fib}(j + k)$
$= \quad \mathbf{if}\ j \simeq \mathtt{0}\ \ \mathbf{then}\ \mathrm{fib}(k)$
$\quad \mathbf{else}\ (\mathrm{fib}(1 + k) * \mathrm{fib}(j)) + (\mathrm{fib}(j - 1) * \mathrm{fib}(k))\ \mathbf{endif}$

THEOREM: gcd-fib-next-fib
$\mathrm{gcd}(\mathrm{fib}(n), \mathrm{fib}(1 + n)) = \mathtt{1}$

THEOREM: gcd-fib
$\mathrm{gcd}(\mathrm{fib}(a), \mathrm{fib}(b)) = \mathrm{fib}(\mathrm{gcd}(a, b))$

THEOREM: equal-fib-constant
$((\mathrm{fib}(a) = \mathtt{0}) = (a \simeq \mathtt{0}))$
$\wedge \quad ((\mathrm{fib}(a) = \mathtt{1}) = ((a = \mathtt{1}) \vee (a = \mathtt{2})))$

THEOREM: fib-small
$(a < \mathtt{3})$
$\rightarrow \quad (\mathrm{fib}(a)$
$\quad = \quad \mathbf{if}\ a \simeq \mathtt{0}\ \ \mathbf{then}\ \mathtt{0}$
$\quad \quad \mathbf{else}\ \mathtt{1}\ \mathbf{endif})$

DEFINITION:
$\text{double-fib-induction}(a, b)$
$= \quad \mathbf{if}\ (a < \mathtt{3}) \vee (b < \mathtt{3})\ \ \mathbf{then}\ \mathbf{t}$
$\quad \mathbf{else}\ \text{double-fib-induction}(a - 1, b - 1)$
$\quad \quad \wedge \quad \text{double-fib-induction}((a - 1) - 1, (b - 1) - 1)\ \mathbf{endif}$

THEOREM: lessp-fib-fib
$(\mathrm{fib}\,(a) < \mathrm{fib}\,(b)) = ((a < b) \land (\neg\,((a = 1) \land (b = 2))))$

THEOREM: remainder-fib-fib-0
$((\mathrm{fib}\,(a) \ \mathbf{mod}\ \mathrm{fib}\,(b)) = 0) = (((a\ \mathbf{mod}\ b) = 0) \lor (b = 2))$

```
;; fib-times-open and fib-add1-times-open apply fib-plus to
;; particular terms in a way that will be useful in the proof
;; of fib-times-special
```

THEOREM: fib-times-open
$$\begin{aligned} &(0 < k)\\ &\to\ (\mathrm{fib}\,(k * n)\\ &\qquad = ((\mathrm{fib}\,(n) * \mathrm{fib}\,(1 + ((k - 1) * n)))\\ &\qquad\quad + (\mathrm{fib}\,(n - 1) * \mathrm{fib}\,((k - 1) * n)))) \end{aligned}$$

EVENT: Disable fib-times-open.

THEOREM: fib-add1-times-open
$$\begin{aligned} &(0 < k)\\ &\to\ (\mathrm{fib}\,(1 + (k * n))\\ &\qquad = ((\mathrm{fib}\,(1 + ((k - 1) * n)) * \mathrm{fib}\,(1 + n))\\ &\qquad\quad + (\mathrm{fib}\,((k - 1) * n) * \mathrm{fib}\,(n)))) \end{aligned}$$

EVENT: Disable fib-add1-times-open.

THEOREM: fib-times-special-step
$$\begin{aligned} &(1 < k)\\ &\to\ (((k * (\mathrm{fib}\,(n) * \exp\,(\mathrm{fib}\,(1 + n),\ k - 1)))\ \mathbf{mod}\ (\mathrm{fib}\,(n) * \mathrm{fib}\,(n)))\\ &\qquad = (((\mathrm{fib}\,(n) * \exp\,(\mathrm{fib}\,(1 + n),\ k - 1))\\ &\qquad\quad + (\mathrm{fib}\,(n - 1)\\ &\qquad\qquad * ((k - 1)\\ &\qquad\qquad\quad * (\mathrm{fib}\,(n)\\ &\qquad\qquad\qquad * \exp\,(\mathrm{fib}\,(1 + n),\ (k - 1) - 1)))))\\ &\qquad\quad \mathbf{mod}\ \ (\mathrm{fib}\,(n) * \mathrm{fib}\,(n)))) \end{aligned}$$

THEOREM: fib-remainder-hack
$(\mathrm{fib}\,(x * y)\ \mathbf{mod}\ \mathrm{fib}\,(x)) = 0$

```
;; We wish the rewriter to use a modulo arithmetic equality to rewrite
;; a term.  Fortunately, we can can construct REMAINDER-FIB-BACKCHAIN
;; to do it the way we wish since the terms are of a specialized form
```

THEOREM: remainder-backchain-proof1
$((a\ \mathbf{mod}\ c) = (b\ \mathbf{mod}\ c)) \to (((a * d)\ \mathbf{mod}\ c) = ((b * d)\ \mathbf{mod}\ c))$

THEOREM: remainder-backchain-proof2
$(((a \textbf{ mod } c) = (b \textbf{ mod } c)) \land ((d \textbf{ mod } c) = (e \textbf{ mod } c)))$
$\rightarrow \quad (((a + d) \textbf{ mod } c) = ((b + e) \textbf{ mod } c))$

THEOREM: remainder-fib-backchain
$(((\text{fib}\,(x) \textbf{ mod } c) = (\exp\,(p,\ q) \textbf{ mod } c))$
$\land \quad ((\text{fib}\,(y) \textbf{ mod } c) = ((r * s) \textbf{ mod } c)))$
$\rightarrow \quad ((((a * \text{fib}\,(x)) + (b * \text{fib}\,(y))) \textbf{ mod } c)$
$= \quad (((a * \exp\,(p,\ q)) + (b * (r * s))) \textbf{ mod } c))$

```
;; This is the guts of the proof
```

THEOREM: fib-times-special
$(1 < k)$
$\rightarrow \quad (((\text{fib}\,(k * n) \textbf{ mod } \exp\,(\text{fib}\,(n),\, 2))$
$= \quad ((k * (\text{fib}\,(n) * \exp\,(\text{fib}\,(1 + n),\ k - 1)))$
$\textbf{mod} \quad \exp\,(\text{fib}\,(n),\, 2)))$
$\land \quad ((\text{fib}\,(1 + (k * n)) \textbf{ mod } \exp\,(\text{fib}\,(n),\, 2))$
$= \quad (\exp\,(\text{fib}\,(1 + n),\ k) \textbf{ mod } \exp\,(\text{fib}\,(n),\, 2))))$

THEOREM: fib-remainder-times-special
$(\text{fib}\,(n * k) \textbf{ mod } (\text{fib}\,(n) * \text{fib}\,(n)))$
$= \quad ((k * (\text{fib}\,(n) * \exp\,(\text{fib}\,(1 + n),\ k - 1))) \textbf{ mod } (\text{fib}\,(n) * \text{fib}\,(n)))$

THEOREM: remainder-times-times-hack2
$((k * n) \textbf{ mod } (n * p)) = (n * (k \textbf{ mod } p))$

THEOREM: matijasevich-lemma-helper
$((2 < n) \land ((m \textbf{ mod } n) = 0))$
$\rightarrow \quad (((\text{fib}\,(m) \textbf{ mod } (\text{fib}\,(n) * \text{fib}\,(n))) = 0)$
$= \quad ((m \textbf{ mod } (n * \text{fib}\,(n))) = 0))$

THEOREM: matijasevich-lemma
$(2 < n)$
$\rightarrow \quad (((\text{fib}\,(m) \textbf{ mod } (\text{fib}\,(n) * \text{fib}\,(n))) = 0)$
$= \quad ((m \textbf{ mod } (n * \text{fib}\,(n))) = 0))$

Index