

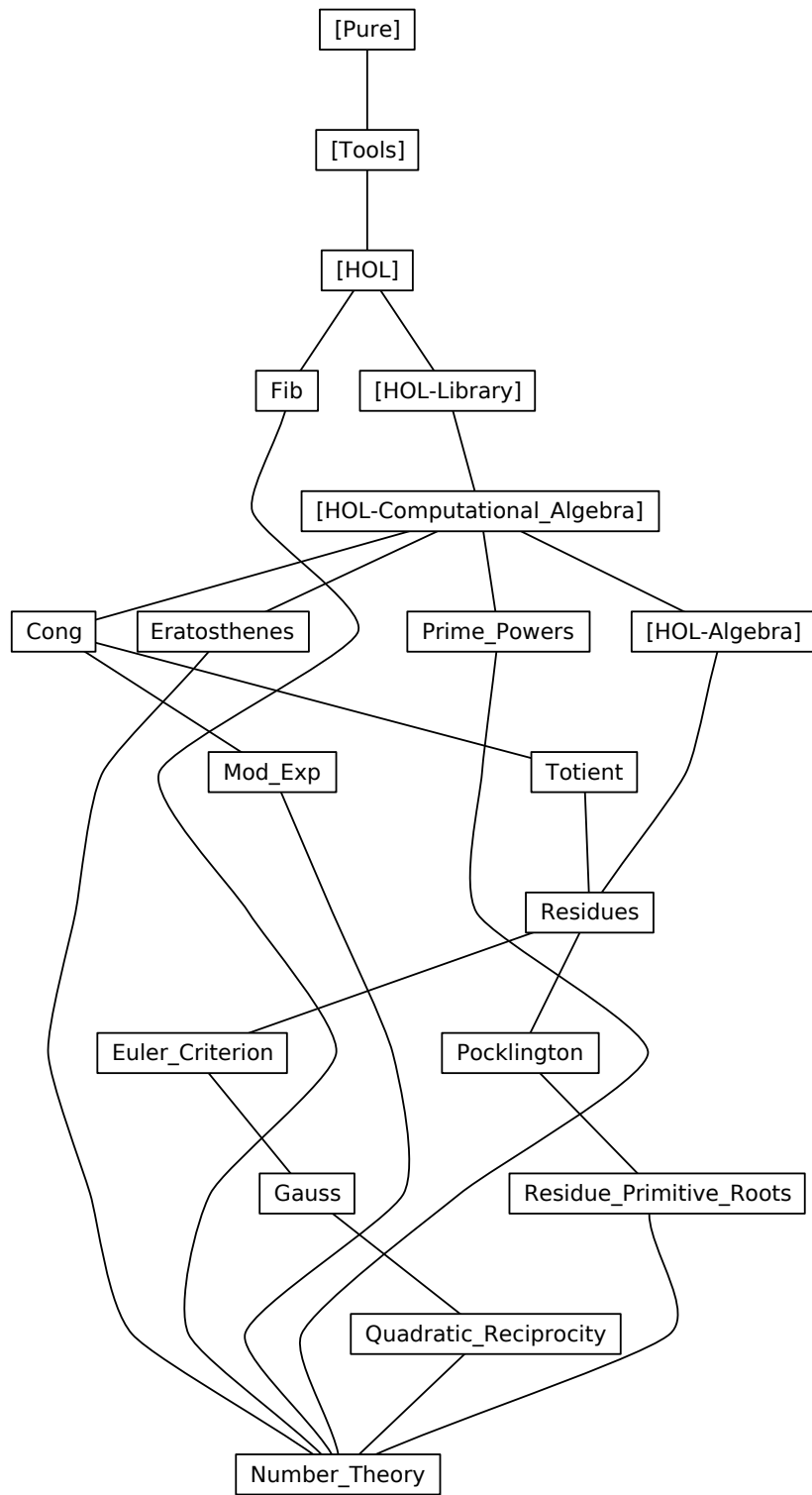
Various results of number theory

December 12, 2021

Contents

1	The fibonacci function	3
1.1	Fibonacci numbers	3
1.2	Basic Properties	3
1.3	More efficient code	3
1.4	A Few Elementary Results	4
1.5	Law 6.111 of Concrete Mathematics	4
1.6	Closed form	5
1.7	Divide-and-Conquer recurrence	5
1.8	Fibonacci and Binomial Coefficients	6
2	Congruence	6
2.1	Generic congruences	6
2.2	Congruences on <i>nat</i> and <i>int</i>	10
3	Fundamental facts about Euler's totient function	15
4	Residue rings	20
4.1	A locale for residue rings	20
4.2	Prime residues	23
5	Test cases: Euler's theorem and Wilson's theorem	24
5.1	Euler's theorem	24
5.2	Wilson's theorem	24
5.3	Upper bound for the number of n -th roots	25
6	The sieve of Eratosthenes	25
6.1	Preliminary: strict divisibility	25
6.2	Main corpus	25
6.3	Application: smallest prime beyond a certain number	28
7	Fast modular exponentiation	29

8	Gauss' Lemma	32
8.1	Basic properties of p	33
8.2	Basic Properties of the Gauss Sets	33
8.3	Relationships Between Gauss Sets	35
8.4	Gauss' Lemma	36
9	Pocklington's Theorem for Primes	40
9.1	Lemmas about previously defined terms	40
9.2	Some basic theorems about solving congruences	41
9.3	Lucas's theorem	41
9.4	Definition of the order of a number mod n	42
9.5	Another trivial primality characterization	45
9.6	Pocklington theorem	45
9.7	Prime factorizations	46
10	Prime powers	47
11	Primitive roots in residue rings and Carmichael's function	52
11.1	Primitive roots in residue rings	52
11.2	Primitive roots modulo a prime	53
11.3	Primitive roots modulo powers of an odd prime	54
11.4	Carmichael's function	55
11.5	Existence of primitive roots for general moduli	57
12	Comprehensive number theory	59



1 The fibonacci function

```
theory Fib
  imports Complex-Main
begin
```

1.1 Fibonacci numbers

```
fun fib :: nat  $\Rightarrow$  nat
  where
    fib0: fib 0 = 0
  | fib1: fib (Suc 0) = 1
  | fib2: fib (Suc (Suc n)) = fib (Suc n) + fib n
```

1.2 Basic Properties

```
lemma fib-1 [simp]: fib 1 = 1
  <proof>
```

```
lemma fib-2 [simp]: fib 2 = 1
  <proof>
```

```
lemma fib-plus-2: fib (n + 2) = fib (n + 1) + fib n
  <proof>
```

```
lemma fib-add: fib (Suc (n + k)) = fib (Suc k) * fib (Suc n) + fib k * fib n
  <proof>
```

```
lemma fib-neq-0-nat: n > 0  $\implies$  fib n > 0
  <proof>
```

```
lemma fib-Suc-mono: fib m  $\leq$  fib (Suc m)
  <proof>
```

```
lemma fib-mono: m  $\leq$  n  $\implies$  fib m  $\leq$  fib n
  <proof>
```

1.3 More efficient code

The naive approach is very inefficient since the branching recursion leads to many values of *fib* being computed multiple times. We can avoid this by “remembering” the last two values in the sequence, yielding a tail-recursive version. This is far from optimal (it takes roughly $O(n \cdot M(n))$ time where $M(n)$ is the time required to multiply two n -bit integers), but much better than the naive version, which is exponential.

```
fun gen-fib :: nat  $\Rightarrow$  nat  $\Rightarrow$  nat  $\Rightarrow$  nat
  where
    gen-fib a b 0 = a
  | gen-fib a b (Suc 0) = b
```

$$| \text{gen-fib } a \ b \ (\text{Suc } (\text{Suc } n)) = \text{gen-fib } b \ (a + b) \ (\text{Suc } n)$$

lemma *gen-fib-recurrence*: $\text{gen-fib } a \ b \ (\text{Suc } (\text{Suc } n)) = \text{gen-fib } a \ b \ n + \text{gen-fib } a \ b \ (\text{Suc } n)$
 ⟨proof⟩

lemma *gen-fib-fib*: $\text{gen-fib } (\text{fib } n) \ (\text{fib } (\text{Suc } n)) \ m = \text{fib } (n + m)$
 ⟨proof⟩

lemma *fib-conv-gen-fib*: $\text{fib } n = \text{gen-fib } 0 \ 1 \ n$
 ⟨proof⟩

declare *fib-conv-gen-fib* [code]

1.4 A Few Elementary Results

Concrete Mathematics, page 278: Cassini's identity. The proof is much easier using integers, not natural numbers!

lemma *fib-Cassini-int*: $\text{int } (\text{fib } (\text{Suc } (\text{Suc } n)) * \text{fib } n) - \text{int } ((\text{fib } (\text{Suc } n))^2) = -((-1)^n)$
 ⟨proof⟩

lemma *fib-Cassini-nat*:
 $\text{fib } (\text{Suc } (\text{Suc } n)) * \text{fib } n =$
 (if even n then $(\text{fib } (\text{Suc } n))^2 - 1$ else $(\text{fib } (\text{Suc } n))^2 + 1$)
 ⟨proof⟩

1.5 Law 6.111 of Concrete Mathematics

lemma *coprime-fib-Suc-nat*: $\text{coprime } (\text{fib } n) \ (\text{fib } (\text{Suc } n))$
 ⟨proof⟩

lemma *gcd-fib-add*:
 $\text{gcd } (\text{fib } m) \ (\text{fib } (n + m)) = \text{gcd } (\text{fib } m) \ (\text{fib } n)$
 ⟨proof⟩

lemma *gcd-fib-diff*: $m \leq n \implies \text{gcd } (\text{fib } m) \ (\text{fib } (n - m)) = \text{gcd } (\text{fib } m) \ (\text{fib } n)$
 ⟨proof⟩

lemma *gcd-fib-mod*: $0 < m \implies \text{gcd } (\text{fib } m) \ (\text{fib } (n \bmod m)) = \text{gcd } (\text{fib } m) \ (\text{fib } n)$
 ⟨proof⟩

lemma *fib-gcd*: $\text{fib } (\text{gcd } m \ n) = \text{gcd } (\text{fib } m) \ (\text{fib } n)$ — Law 6.111
 ⟨proof⟩

theorem *fib-mult-eq-sum-nat*: $\text{fib } (\text{Suc } n) * \text{fib } n = (\sum k \in \{..n\}. \text{fib } k * \text{fib } k)$
 ⟨proof⟩

1.6 Closed form

lemma *fib-closed-form*:

```

fixes  $\varphi \ \psi :: \text{real}$ 
defines  $\varphi \equiv (1 + \text{sqrt } 5) / 2$ 
and  $\psi \equiv (1 - \text{sqrt } 5) / 2$ 
shows  $\text{of-nat } (\text{fib } n) = (\varphi ^ n - \psi ^ n) / \text{sqrt } 5$ 
<proof>

```

lemma *fib-closed-form'*:

```

fixes  $\varphi \ \psi :: \text{real}$ 
defines  $\varphi \equiv (1 + \text{sqrt } 5) / 2$ 
and  $\psi \equiv (1 - \text{sqrt } 5) / 2$ 
assumes  $n > 0$ 
shows  $\text{fib } n = \text{round } (\varphi ^ n / \text{sqrt } 5)$ 
<proof>

```

lemma *fib-asymptotics*:

```

fixes  $\varphi :: \text{real}$ 
defines  $\varphi \equiv (1 + \text{sqrt } 5) / 2$ 
shows  $(\lambda n. \text{real } (\text{fib } n) / (\varphi ^ n / \text{sqrt } 5)) \longrightarrow 1$ 
<proof>

```

1.7 Divide-and-Conquer recurrence

The following divide-and-conquer recurrence allows for a more efficient computation of Fibonacci numbers; however, it requires memoisation of values to be reasonably efficient, cutting the number of values to be computed to logarithmically many instead of linearly many. The vast majority of the computation time is then actually spent on the multiplication, since the output number is exponential in the input number.

lemma *fib-rec-odd*:

```

fixes  $\varphi \ \psi :: \text{real}$ 
defines  $\varphi \equiv (1 + \text{sqrt } 5) / 2$ 
and  $\psi \equiv (1 - \text{sqrt } 5) / 2$ 
shows  $\text{fib } (\text{Suc } (2 * n)) = \text{fib } n ^ 2 + \text{fib } (\text{Suc } n) ^ 2$ 
<proof>

```

lemma *fib-rec-even*: $\text{fib } (2 * n) = (\text{fib } (n - 1) + \text{fib } (n + 1)) * \text{fib } n$

<proof>

lemma *fib-rec-even'*: $\text{fib } (2 * n) = (2 * \text{fib } (n - 1) + \text{fib } n) * \text{fib } n$

<proof>

lemma *fib-rec*:

```

fib  $n =$ 
  (if  $n = 0$  then 0 else if  $n = 1$  then 1
   else if even  $n$  then let  $n' = n \text{ div } 2$ ;  $fn = \text{fib } n'$  in  $(2 * \text{fib } (n' - 1) + fn) * fn$ 
   else let  $n' = n \text{ div } 2$  in  $\text{fib } n' ^ 2 + \text{fib } (\text{Suc } n') ^ 2$ )

```

$\langle proof \rangle$

1.8 Fibonacci and Binomial Coefficients

lemma *sum-drop-zero*: $(\sum k = 0..Suc\ n. \text{ if } 0 < k \text{ then } (f\ (k - 1)) \text{ else } 0) = (\sum j = 0..n. f\ j)$
 $\langle proof \rangle$

lemma *sum-choose-drop-zero*:
 $(\sum k = 0..Suc\ n. \text{ if } k = 0 \text{ then } 0 \text{ else } (Suc\ n - k) \text{ choose } (k - 1)) =$
 $(\sum j = 0..n. (n-j) \text{ choose } j)$
 $\langle proof \rangle$

lemma *ne-diagonal-fib*: $(\sum k = 0..n. (n-k) \text{ choose } k) = fib\ (Suc\ n)$
 $\langle proof \rangle$

end

2 Congruence

theory *Cong*
imports *HOL-Computational-Algebra.Primes*
begin

2.1 Generic congruences

context *unique-euclidean-semiring*
begin

definition *cong* :: $'a \Rightarrow 'a \Rightarrow 'a \Rightarrow bool$ $(\langle (1[- = -] \ '(\text{' mod } -)) \rangle)$
where $cong\ b\ c\ a \longleftrightarrow b\ mod\ a = c\ mod\ a$

abbreviation *notcong* :: $'a \Rightarrow 'a \Rightarrow 'a \Rightarrow bool$ $(\langle (1[- \neq -] \ '(\text{' mod } -)) \rangle)$
where $notcong\ b\ c\ a \equiv \neg\ cong\ b\ c\ a$

lemma *cong-refl* [*simp*]:
 $[b = b] \ (mod\ a)$
 $\langle proof \rangle$

lemma *cong-sym*:
 $[b = c] \ (mod\ a) \implies [c = b] \ (mod\ a)$
 $\langle proof \rangle$

lemma *cong-sym-eq*:
 $[b = c] \ (mod\ a) \longleftrightarrow [c = b] \ (mod\ a)$
 $\langle proof \rangle$

lemma *cong-trans* [*trans*]:
 $[b = c] \ (mod\ a) \implies [c = d] \ (mod\ a) \implies [b = d] \ (mod\ a)$

$\langle proof \rangle$

lemma *cong-mult-self-right*:

$[b * a = 0] \text{ (mod } a)$

$\langle proof \rangle$

lemma *cong-mult-self-left*:

$[a * b = 0] \text{ (mod } a)$

$\langle proof \rangle$

lemma *cong-mod-left* [*simp*]:

$[b \text{ mod } a = c] \text{ (mod } a) \longleftrightarrow [b = c] \text{ (mod } a)$

$\langle proof \rangle$

lemma *cong-mod-right* [*simp*]:

$[b = c \text{ mod } a] \text{ (mod } a) \longleftrightarrow [b = c] \text{ (mod } a)$

$\langle proof \rangle$

lemma *cong-0* [*simp*, *presburger*]:

$[b = c] \text{ (mod } 0) \longleftrightarrow b = c$

$\langle proof \rangle$

lemma *cong-1* [*simp*, *presburger*]:

$[b = c] \text{ (mod } 1)$

$\langle proof \rangle$

lemma *cong-dvd-iff*:

$a \text{ dvd } b \longleftrightarrow a \text{ dvd } c \text{ if } [b = c] \text{ (mod } a)$

$\langle proof \rangle$

lemma *cong-0-iff*: $[b = 0] \text{ (mod } a) \longleftrightarrow a \text{ dvd } b$

$\langle proof \rangle$

lemma *cong-add*:

$[b = c] \text{ (mod } a) \implies [d = e] \text{ (mod } a) \implies [b + d = c + e] \text{ (mod } a)$

$\langle proof \rangle$

lemma *cong-mult*:

$[b = c] \text{ (mod } a) \implies [d = e] \text{ (mod } a) \implies [b * d = c * e] \text{ (mod } a)$

$\langle proof \rangle$

lemma *cong-scalar-right*:

$[b = c] \text{ (mod } a) \implies [b * d = c * d] \text{ (mod } a)$

$\langle proof \rangle$

lemma *cong-scalar-left*:

$[b = c] \text{ (mod } a) \implies [d * b = d * c] \text{ (mod } a)$

$\langle proof \rangle$

lemma *cong-pow*:

$$[b = c] \text{ (mod } a) \implies [b \wedge n = c \wedge n] \text{ (mod } a)$$

<proof>

lemma *cong-sum*:

$$[\text{sum } f \ A = \text{sum } g \ A] \text{ (mod } a) \text{ if } \bigwedge x. x \in A \implies [f \ x = g \ x] \text{ (mod } a)$$

<proof>

lemma *cong-prod*:

$$[\text{prod } f \ A = \text{prod } g \ A] \text{ (mod } a) \text{ if } (\bigwedge x. x \in A \implies [f \ x = g \ x] \text{ (mod } a))$$

<proof>

lemma *mod-mult-cong-right*:

$$[c \text{ mod } (a * b) = d] \text{ (mod } a) \longleftrightarrow [c = d] \text{ (mod } a)$$

<proof>

lemma *mod-mult-cong-left*:

$$[c \text{ mod } (b * a) = d] \text{ (mod } a) \longleftrightarrow [c = d] \text{ (mod } a)$$

<proof>

end

context *unique-euclidean-ring*

begin

lemma *cong-diff*:

$$[b = c] \text{ (mod } a) \implies [d = e] \text{ (mod } a) \implies [b - d = c - e] \text{ (mod } a)$$

<proof>

lemma *cong-diff-iff-cong-0*:

$$[b - c = 0] \text{ (mod } a) \longleftrightarrow [b = c] \text{ (mod } a) \text{ (is } ?P \longleftrightarrow ?Q)$$

<proof>

lemma *cong-minus-minus-iff*:

$$[- \ b = - \ c] \text{ (mod } a) \longleftrightarrow [b = c] \text{ (mod } a)$$

<proof>

lemma *cong-modulus-minus-iff* [*iff*]:

$$[b = c] \text{ (mod } - \ a) \longleftrightarrow [b = c] \text{ (mod } a)$$

<proof>

lemma *cong-iff-dvd-diff*:

$$[a = b] \text{ (mod } m) \longleftrightarrow m \text{ dvd } (a - b)$$

<proof>

lemma *cong-iff-lin*:

$$[a = b] \text{ (mod } m) \longleftrightarrow (\exists k. b = a + m * k) \text{ (is } ?P \longleftrightarrow ?Q)$$

<proof>

lemma *cong-add-lcancel*:

$$[a + x = a + y] \text{ (mod } n) \longleftrightarrow [x = y] \text{ (mod } n)$$

<proof>

lemma *cong-add-rcancel*:

$$[x + a = y + a] \text{ (mod } n) \longleftrightarrow [x = y] \text{ (mod } n)$$

<proof>

lemma *cong-add-lcancel-0*:

$$[a + x = a] \text{ (mod } n) \longleftrightarrow [x = 0] \text{ (mod } n)$$

<proof>

lemma *cong-add-rcancel-0*:

$$[x + a = a] \text{ (mod } n) \longleftrightarrow [x = 0] \text{ (mod } n)$$

<proof>

lemma *cong-dvd-modulus*:

$$[x = y] \text{ (mod } n) \text{ if } [x = y] \text{ (mod } m) \text{ and } n \text{ dvd } m$$

<proof>

lemma *cong-modulus-mult*:

$$[x = y] \text{ (mod } m) \text{ if } [x = y] \text{ (mod } m * n)$$

<proof>

end

lemma *cong-abs [simp]*:

$$[x = y] \text{ (mod } |m|) \longleftrightarrow [x = y] \text{ (mod } m)$$

for $x\ y :: 'a :: \{\text{unique-euclidean-ring, linordered-idom}\}$

<proof>

lemma *cong-square*:

$$\text{prime } p \implies 0 < a \implies [a * a = 1] \text{ (mod } p) \implies [a = 1] \text{ (mod } p) \vee [a = -1] \text{ (mod } p)$$

for $a\ p :: 'a :: \{\text{normalization-semidom, linordered-idom, unique-euclidean-ring}\}$

<proof>

lemma *cong-mult-rcancel*:

$$[a * k = b * k] \text{ (mod } m) \longleftrightarrow [a = b] \text{ (mod } m)$$

if *coprime* $k\ m$ **for** $a\ k\ m :: 'a :: \{\text{unique-euclidean-ring, ring-gcd}\}$

<proof>

lemma *cong-mult-lcancel*:

$$[k * a = k * b] \text{ (mod } m) = [a = b] \text{ (mod } m)$$

if *coprime* $k\ m$ **for** $a\ k\ m :: 'a :: \{\text{unique-euclidean-ring, ring-gcd}\}$

<proof>

lemma *coprime-cong-mult*:

$$[a = b] \text{ (mod } m) \implies [a = b] \text{ (mod } n) \implies \text{coprime } m\ n \implies [a = b] \text{ (mod } m * n)$$

for $a\ b :: 'a :: \{\text{unique-euclidean-ring}, \text{semiring-gcd}\}$
 $\langle \text{proof} \rangle$

lemma *cong-gcd-eq*:

$\text{gcd } a\ m = \text{gcd } b\ m$ **if** $[a = b] \ (\text{mod } m)$
for $a\ b :: 'a :: \{\text{unique-euclidean-semiring}, \text{euclidean-semiring-gcd}\}$
 $\langle \text{proof} \rangle$

lemma *cong-imp-coprime*:

$[a = b] \ (\text{mod } m) \implies \text{coprime } a\ m \implies \text{coprime } b\ m$
for $a\ b :: 'a :: \{\text{unique-euclidean-semiring}, \text{euclidean-semiring-gcd}\}$
 $\langle \text{proof} \rangle$

lemma *cong-cong-prod-coprime*:

$[x = y] \ (\text{mod } (\prod_{i \in A} m\ i))$ **if**
 $(\forall i \in A. [x = y] \ (\text{mod } m\ i))$
 $(\forall i \in A. (\forall j \in A. i \neq j \longrightarrow \text{coprime } (m\ i) \ (m\ j)))$
for $x\ y :: 'a :: \{\text{unique-euclidean-ring}, \text{semiring-gcd}\}$
 $\langle \text{proof} \rangle$

2.2 Congruences on *nat* and *int*

lemma *cong-int-iff*:

$[\text{int } m = \text{int } q] \ (\text{mod } \text{int } n) \longleftrightarrow [m = q] \ (\text{mod } n)$
 $\langle \text{proof} \rangle$

lemma *cong-Suc-0* [*simp*, *presburger*]:

$[m = n] \ (\text{mod } \text{Suc } 0)$
 $\langle \text{proof} \rangle$

lemma *cong-diff-nat*:

$[a - c = b - d] \ (\text{mod } m)$ **if** $[a = b] \ (\text{mod } m)$ $[c = d] \ (\text{mod } m)$
and $a \geq c$ $b \geq d$ **for** $a\ b\ c\ d\ m :: \text{nat}$
 $\langle \text{proof} \rangle$

lemma *cong-diff-iff-cong-0-nat*:

$[a - b = 0] \ (\text{mod } m) \longleftrightarrow [a = b] \ (\text{mod } m)$ **if** $a \geq b$ **for** $a\ b :: \text{nat}$
 $\langle \text{proof} \rangle$

lemma *cong-diff-iff-cong-0-nat'*:

$[\text{nat } |\text{int } a - \text{int } b| = 0] \ (\text{mod } m) \longleftrightarrow [a = b] \ (\text{mod } m)$
 $\langle \text{proof} \rangle$

lemma *cong-altdef-nat*:

$a \geq b \implies [a = b] \ (\text{mod } m) \longleftrightarrow m \text{ dvd } (a - b)$
for $a\ b :: \text{nat}$
 $\langle \text{proof} \rangle$

lemma *cong-altdef-nat'*:

$[a = b] \text{ (mod } m) \longleftrightarrow m \text{ dvd nat } | \text{int } a - \text{int } b |$
 $\langle \text{proof} \rangle$

lemma *cong-mult-rcancel-nat*:
 $[a * k = b * k] \text{ (mod } m) \longleftrightarrow [a = b] \text{ (mod } m)$
if *coprime* *k m* **for** *a k m :: nat*
 $\langle \text{proof} \rangle$

lemma *cong-mult-lcancel-nat*:
 $[k * a = k * b] \text{ (mod } m) = [a = b] \text{ (mod } m)$
if *coprime* *k m* **for** *a k m :: nat*
 $\langle \text{proof} \rangle$

lemma *coprime-cong-mult-nat*:
 $[a = b] \text{ (mod } m) \implies [a = b] \text{ (mod } n) \implies \text{coprime } m \ n \implies [a = b] \text{ (mod } m * n)$
for *a b :: nat*
 $\langle \text{proof} \rangle$

lemma *cong-less-imp-eq-nat*: $0 \leq a \implies a < m \implies 0 \leq b \implies b < m \implies [a = b] \text{ (mod } m) \implies a = b$
for *a b :: nat*
 $\langle \text{proof} \rangle$

lemma *cong-less-imp-eq-int*: $0 \leq a \implies a < m \implies 0 \leq b \implies b < m \implies [a = b] \text{ (mod } m) \implies a = b$
for *a b :: int*
 $\langle \text{proof} \rangle$

lemma *cong-less-unique-nat*: $0 < m \implies (\exists ! b. 0 \leq b \wedge b < m \wedge [a = b] \text{ (mod } m))$
for *a m :: nat*
 $\langle \text{proof} \rangle$

lemma *cong-less-unique-int*: $0 < m \implies (\exists ! b. 0 \leq b \wedge b < m \wedge [a = b] \text{ (mod } m))$
for *a m :: int*
 $\langle \text{proof} \rangle$

lemma *cong-iff-lin-nat*: $([a = b] \text{ (mod } m)) \longleftrightarrow (\exists k1 \ k2. b + k1 * m = a + k2 * m)$
(is ?lhs = ?rhs)
for *a b :: nat*
 $\langle \text{proof} \rangle$

lemma *cong-cong-mod-nat*: $[a = b] \text{ (mod } m) \longleftrightarrow [a \text{ mod } m = b \text{ mod } m] \text{ (mod } m)$
for *a b :: nat*
 $\langle \text{proof} \rangle$

lemma *cong-cong-mod-int*: $[a = b] \text{ (mod } m) \longleftrightarrow [a \text{ mod } m = b \text{ mod } m] \text{ (mod } m)$
for *a b :: int*

$\langle proof \rangle$

lemma *cong-add-lcancel-nat*: $[a + x = a + y] \text{ (mod } n) \longleftrightarrow [x = y] \text{ (mod } n)$
for $a \ x \ y :: \text{nat}$
 $\langle proof \rangle$

lemma *cong-add-rcancel-nat*: $[x + a = y + a] \text{ (mod } n) \longleftrightarrow [x = y] \text{ (mod } n)$
for $a \ x \ y :: \text{nat}$
 $\langle proof \rangle$

lemma *cong-add-lcancel-0-nat*: $[a + x = a] \text{ (mod } n) \longleftrightarrow [x = 0] \text{ (mod } n)$
for $a \ x :: \text{nat}$
 $\langle proof \rangle$

lemma *cong-add-rcancel-0-nat*: $[x + a = a] \text{ (mod } n) \longleftrightarrow [x = 0] \text{ (mod } n)$
for $a \ x :: \text{nat}$
 $\langle proof \rangle$

lemma *cong-dvd-modulus-nat*: $[x = y] \text{ (mod } m) \implies n \text{ dvd } m \implies [x = y] \text{ (mod } n)$
for $x \ y :: \text{nat}$
 $\langle proof \rangle$

lemma *cong-to-1-nat*:
fixes $a :: \text{nat}$
assumes $[a = 1] \text{ (mod } n)$
shows $n \text{ dvd } (a - 1)$
 $\langle proof \rangle$

lemma *cong-0-1-nat'*: $[0 = \text{Suc } 0] \text{ (mod } n) \longleftrightarrow n = \text{Suc } 0$
 $\langle proof \rangle$

lemma *cong-0-1-nat*: $[0 = 1] \text{ (mod } n) \longleftrightarrow n = 1$
for $n :: \text{nat}$
 $\langle proof \rangle$

lemma *cong-0-1-int*: $[0 = 1] \text{ (mod } n) \longleftrightarrow n = 1 \vee n = -1$
for $n :: \text{int}$
 $\langle proof \rangle$

lemma *cong-to-1'-nat*: $[a = 1] \text{ (mod } n) \longleftrightarrow a = 0 \wedge n = 1 \vee (\exists m. a = 1 + m * n)$
for $a :: \text{nat}$
 $\langle proof \rangle$

lemma *cong-le-nat*: $y \leq x \implies [x = y] \text{ (mod } n) \longleftrightarrow (\exists q. x = q * n + y)$
for $x \ y :: \text{nat}$
 $\langle proof \rangle$

lemma *cong-solve-nat*:
fixes $a :: \text{nat}$
shows $\exists x. [a * x = \text{gcd } a \ n] \ (\text{mod } n)$
 $\langle \text{proof} \rangle$

lemma *cong-solve-int*:
fixes $a :: \text{int}$
shows $\exists x. [a * x = \text{gcd } a \ n] \ (\text{mod } n)$
 $\langle \text{proof} \rangle$

lemma *cong-solve-dvd-nat*:
fixes $a :: \text{nat}$
assumes $\text{gcd } a \ n \ \text{dvd } d$
shows $\exists x. [a * x = d] \ (\text{mod } n)$
 $\langle \text{proof} \rangle$

lemma *cong-solve-dvd-int*:
fixes $a :: \text{int}$
assumes $b: \text{gcd } a \ n \ \text{dvd } d$
shows $\exists x. [a * x = d] \ (\text{mod } n)$
 $\langle \text{proof} \rangle$

lemma *cong-solve-coprime-nat*:
 $\exists x. [a * x = \text{Suc } 0] \ (\text{mod } n)$ **if** $\text{coprime } a \ n$
 $\langle \text{proof} \rangle$

lemma *cong-solve-coprime-int*:
 $\exists x. [a * x = 1] \ (\text{mod } n)$ **if** $\text{coprime } a \ n$ **for** $a \ n \ x :: \text{int}$
 $\langle \text{proof} \rangle$

lemma *coprime-iff-invertible-nat*:
 $\text{coprime } a \ m \longleftrightarrow (\exists x. [a * x = \text{Suc } 0] \ (\text{mod } m))$ **(is** $?P \longleftrightarrow ?Q$ **)**
 $\langle \text{proof} \rangle$

lemma *coprime-iff-invertible-int*:
 $\text{coprime } a \ m \longleftrightarrow (\exists x. [a * x = 1] \ (\text{mod } m))$ **(is** $?P \longleftrightarrow ?Q$ **) for** $m :: \text{int}$
 $\langle \text{proof} \rangle$

lemma *coprime-iff-invertible'-nat*:
assumes $m > 0$
shows $\text{coprime } a \ m \longleftrightarrow (\exists x. 0 \leq x \wedge x < m \wedge [a * x = \text{Suc } 0] \ (\text{mod } m))$
 $\langle \text{proof} \rangle$

lemma *coprime-iff-invertible'-int*:
fixes $m :: \text{int}$
assumes $m > 0$
shows $\text{coprime } a \ m \longleftrightarrow (\exists x. 0 \leq x \wedge x < m \wedge [a * x = 1] \ (\text{mod } m))$
 $\langle \text{proof} \rangle$

lemma *cong-cong-lcm-nat*: $[x = y] \text{ (mod } a) \implies [x = y] \text{ (mod } b) \implies [x = y] \text{ (mod lcm } a \text{ } b)$

for $x \ y :: \text{nat}$
 $\langle \text{proof} \rangle$

lemma *cong-cong-lcm-int*: $[x = y] \text{ (mod } a) \implies [x = y] \text{ (mod } b) \implies [x = y] \text{ (mod lcm } a \text{ } b)$

for $x \ y :: \text{int}$
 $\langle \text{proof} \rangle$

lemma *cong-cong-prod-coprime-nat*:

$[x = y] \text{ (mod } (\prod_{i \in A} m \ i))$ **if**
 $(\forall i \in A. [x = y] \text{ (mod } m \ i))$
 $(\forall i \in A. (\forall j \in A. i \neq j \longrightarrow \text{coprime } (m \ i) (m \ j)))$
for $x \ y :: \text{nat}$
 $\langle \text{proof} \rangle$

lemma *binary-chinese-remainder-nat*:

fixes $m1 \ m2 :: \text{nat}$
assumes $a: \text{coprime } m1 \ m2$
shows $\exists x. [x = u1] \text{ (mod } m1) \wedge [x = u2] \text{ (mod } m2)$
 $\langle \text{proof} \rangle$

lemma *binary-chinese-remainder-int*:

fixes $m1 \ m2 :: \text{int}$
assumes $a: \text{coprime } m1 \ m2$
shows $\exists x. [x = u1] \text{ (mod } m1) \wedge [x = u2] \text{ (mod } m2)$
 $\langle \text{proof} \rangle$

lemma *cong-modulus-mult-nat*: $[x = y] \text{ (mod } m * n) \implies [x = y] \text{ (mod } m)$

for $x \ y :: \text{nat}$
 $\langle \text{proof} \rangle$

lemma *cong-less-modulus-unique-nat*: $[x = y] \text{ (mod } m) \implies x < m \implies y < m \implies$

$x = y$
for $x \ y :: \text{nat}$
 $\langle \text{proof} \rangle$

lemma *binary-chinese-remainder-unique-nat*:

fixes $m1 \ m2 :: \text{nat}$
assumes $a: \text{coprime } m1 \ m2$
and $\text{nz}: m1 \neq 0 \ m2 \neq 0$
shows $\exists! x. x < m1 * m2 \wedge [x = u1] \text{ (mod } m1) \wedge [x = u2] \text{ (mod } m2)$
 $\langle \text{proof} \rangle$

lemma *chinese-remainder-nat*:

fixes $A :: 'a \text{ set}$
and $m :: 'a \Rightarrow \text{nat}$
and $u :: 'a \Rightarrow \text{nat}$

assumes *fin*: *finite A*
and *cop*: $\forall i \in A. \forall j \in A. i \neq j \longrightarrow \text{coprime } (m \ i) \ (m \ j)$
shows $\exists x. \forall i \in A. [x = u \ i] \ (\text{mod } m \ i)$
 $\langle \text{proof} \rangle$

lemma *coprime-cong-prod-nat*: $[x = y] \ (\text{mod } (\prod_{i \in A} m \ i))$
if $\bigwedge i \ j. [i \in A; j \in A; i \neq j] \implies \text{coprime } (m \ i) \ (m \ j)$
and $\bigwedge i. i \in A \implies [x = y] \ (\text{mod } m \ i)$ **for** $x \ y :: \text{nat}$
 $\langle \text{proof} \rangle$

lemma *chinese-remainder-unique-nat*:
fixes $A :: 'a \text{ set}$
and $m :: 'a \Rightarrow \text{nat}$
and $u :: 'a \Rightarrow \text{nat}$
assumes *fin*: *finite A*
and *nz*: $\forall i \in A. m \ i \neq 0$
and *cop*: $\forall i \in A. \forall j \in A. i \neq j \longrightarrow \text{coprime } (m \ i) \ (m \ j)$
shows $\exists! x. x < (\prod_{i \in A} m \ i) \wedge (\forall i \in A. [x = u \ i] \ (\text{mod } m \ i))$
 $\langle \text{proof} \rangle$

end

3 Fundamental facts about Euler's totient function

theory *Totient*
imports
Complex-Main
HOL-Computational-Algebra.Primes
Cong
begin

definition *totatives* :: $\text{nat} \Rightarrow \text{nat set}$ **where**
 $\text{totatives } n = \{k \in \{0 <..n\}. \text{coprime } k \ n\}$

lemma *in-totatives-iff*: $k \in \text{totatives } n \longleftrightarrow k > 0 \wedge k \leq n \wedge \text{coprime } k \ n$
 $\langle \text{proof} \rangle$

lemma *totatives-code* [*code*]: $\text{totatives } n = \text{Set.filter } (\lambda k. \text{coprime } k \ n) \ \{0 <..n\}$
 $\langle \text{proof} \rangle$

lemma *finite-totatives* [*simp*]: *finite (totatives n)*
 $\langle \text{proof} \rangle$

lemma *totatives-subset*: $\text{totatives } n \subseteq \{0 <..n\}$
 $\langle \text{proof} \rangle$

lemma *zero-not-in-totatives* [*simp*]: $0 \notin \text{totatives } n$

$\langle proof \rangle$

lemma *totatives-le*: $x \in \text{totatives } n \implies x \leq n$
 $\langle proof \rangle$

lemma *totatives-less*:
 assumes $x \in \text{totatives } n \ n > 1$
 shows $x < n$
 $\langle proof \rangle$

lemma *totatives-0* [simp]: $\text{totatives } 0 = \{\}$
 $\langle proof \rangle$

lemma *totatives-1* [simp]: $\text{totatives } 1 = \{\text{Suc } 0\}$
 $\langle proof \rangle$

lemma *totatives-Suc-0* [simp]: $\text{totatives } (\text{Suc } 0) = \{\text{Suc } 0\}$
 $\langle proof \rangle$

lemma *one-in-totatives* [simp]: $n > 0 \implies \text{Suc } 0 \in \text{totatives } n$
 $\langle proof \rangle$

lemma *totatives-eq-empty-iff* [simp]: $\text{totatives } n = \{\} \longleftrightarrow n = 0$
 $\langle proof \rangle$

lemma *minus-one-in-totatives*:
 assumes $n \geq 2$
 shows $n - 1 \in \text{totatives } n$
 $\langle proof \rangle$

lemma *power-in-totatives*:
 assumes $m > 1$ *coprime* $m \ g$
 shows $g^i \bmod m \in \text{totatives } m$
 $\langle proof \rangle$

lemma *totatives-prime-power-Suc*:
 assumes *prime* p
 shows $\text{totatives } (p^i \bmod \text{Suc } n) = \{0 <.. p^i \bmod \text{Suc } n\} - (\lambda m. p * m) ` \{0 <.. p^i \bmod n\}$
 $\langle proof \rangle$

lemma *totatives-prime*: *prime* $p \implies \text{totatives } p = \{0 <.. < p\}$
 $\langle proof \rangle$

lemma *bij-betw-totatives*:
 assumes $m1 > 1 \ m2 > 1$ *coprime* $m1 \ m2$
 shows $\text{bij-betw } (\lambda x. (x \bmod m1, x \bmod m2)) (\text{totatives } (m1 * m2))$
 $(\text{totatives } m1 \times \text{totatives } m2)$
 $\langle proof \rangle$

lemma *bij-betw-totatives-gcd-eq*:

fixes $n\ d :: \text{nat}$

assumes $d\ \text{dvd}\ n\ n > 0$

shows $\text{bij-betw } (\lambda k. k * d) (\text{totatives } (n\ \text{div}\ d)) \{k \in \{0 <..n\}. \text{gcd } k\ n = d\}$

$\langle \text{proof} \rangle$

definition *totient* $:: \text{nat} \Rightarrow \text{nat}$ **where**

$\text{totient } n = \text{card } (\text{totatives } n)$

primrec *totient-naive* $:: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat}$ **where**

$\text{totient-naive } 0\ \text{acc}\ n = \text{acc}$

| $\text{totient-naive } (\text{Suc } k)\ \text{acc}\ n =$

$(\text{if } \text{coprime } (\text{Suc } k)\ n \text{ then } \text{totient-naive } k\ (\text{acc} + 1)\ n \text{ else } \text{totient-naive } k\ \text{acc}\ n)$

lemma *totient-naive*:

$\text{totient-naive } k\ \text{acc}\ n = \text{card } \{x \in \{0 <..k\}. \text{coprime } x\ n\} + \text{acc}$

$\langle \text{proof} \rangle$

lemma *totient-code-naive* [code]: $\text{totient } n = \text{totient-naive } n\ 0\ n$

$\langle \text{proof} \rangle$

lemma *totient-le*: $\text{totient } n \leq n$

$\langle \text{proof} \rangle$

lemma *totient-less*:

assumes $n > 1$

shows $\text{totient } n < n$

$\langle \text{proof} \rangle$

lemma *totient-0* [simp]: $\text{totient } 0 = 0$

$\langle \text{proof} \rangle$

lemma *totient-Suc-0* [simp]: $\text{totient } (\text{Suc } 0) = \text{Suc } 0$

$\langle \text{proof} \rangle$

lemma *totient-1* [simp]: $\text{totient } 1 = \text{Suc } 0$

$\langle \text{proof} \rangle$

lemma *totient-0-iff* [simp]: $\text{totient } n = 0 \longleftrightarrow n = 0$

$\langle \text{proof} \rangle$

lemma *totient-gt-0-iff* [simp]: $\text{totient } n > 0 \longleftrightarrow n > 0$

$\langle \text{proof} \rangle$

lemma *totient-gt-1*:

assumes $n > 2$

shows $\text{totient } n > 1$

$\langle \text{proof} \rangle$

lemma *card-gcd-eq-totient*:
 $n > 0 \implies d \text{ dvd } n \implies \text{card } \{k \in \{0 < .. n\}. \text{gcd } k \ n = d\} = \text{totient } (n \text{ div } d)$
 $\langle \text{proof} \rangle$

lemma *totient-divisor-sum*: $(\sum d \mid d \text{ dvd } n. \text{totient } d) = n$
 $\langle \text{proof} \rangle$

lemma *totient-mult-coprime*:
assumes *coprime* $m \ n$
shows $\text{totient } (m * n) = \text{totient } m * \text{totient } n$
 $\langle \text{proof} \rangle$

lemma *totient-prime-power-Suc*:
assumes *prime* p
shows $\text{totient } (p \wedge \text{Suc } n) = p \wedge n * (p - 1)$
 $\langle \text{proof} \rangle$

lemma *totient-prime-power*:
assumes *prime* $p \ n > 0$
shows $\text{totient } (p \wedge n) = p \wedge (n - 1) * (p - 1)$
 $\langle \text{proof} \rangle$

lemma *totient-imp-prime*:
assumes $\text{totient } p = p - 1 \ p > 0$
shows *prime* p
 $\langle \text{proof} \rangle$

lemma *totient-prime*:
assumes *prime* p
shows $\text{totient } p = p - 1$
 $\langle \text{proof} \rangle$

lemma *totient-2* [simp]: $\text{totient } 2 = 1$
and *totient-3* [simp]: $\text{totient } 3 = 2$
and *totient-5* [simp]: $\text{totient } 5 = 4$
and *totient-7* [simp]: $\text{totient } 7 = 6$
 $\langle \text{proof} \rangle$

lemma *totient-4* [simp]: $\text{totient } 4 = 2$
and *totient-8* [simp]: $\text{totient } 8 = 4$
and *totient-9* [simp]: $\text{totient } 9 = 6$
 $\langle \text{proof} \rangle$

lemma *totient-6* [simp]: $\text{totient } 6 = 2$
 $\langle \text{proof} \rangle$

lemma *totient-even*:
assumes $n > 2$

shows $\text{even } (\text{totient } n)$
 $\langle \text{proof} \rangle$

lemma *totient-prod-coprime*:
assumes $\text{pairwise coprime } (f \text{ ` } A) \text{ inj-on } f \ A$
shows $\text{totient } (\text{prod } f \ A) = (\prod_{a \in A}. \text{totient } (f \ a))$
 $\langle \text{proof} \rangle$

lemma *prime-power-eq-imp-eq*:
fixes $p \ q :: 'a :: \text{factorial-semiring}$
assumes $\text{prime } p \ \text{prime } q \ m > 0$
assumes $p \wedge^m = q \wedge^n$
shows $p = q$
 $\langle \text{proof} \rangle$

lemma *totient-formula1*:
assumes $n > 0$
shows $\text{totient } n = (\prod_{p \in \text{prime-factors } n}. p \wedge^{(\text{multiplicity } p \ n - 1) * (p - 1)})$
 $\langle \text{proof} \rangle$

lemma *totient-dvd*:
assumes $m \ \text{dvd } n$
shows $\text{totient } m \ \text{dvd } \text{totient } n$
 $\langle \text{proof} \rangle$

lemma *totient-dvd-mono*:
assumes $m \ \text{dvd } n \ n > 0$
shows $\text{totient } m \leq \text{totient } n$
 $\langle \text{proof} \rangle$

lemma *prime-factors-power*: $n > 0 \implies \text{prime-factors } (x \wedge^n) = \text{prime-factors } x$
 $\langle \text{proof} \rangle$

lemma *totient-formula2*:
 $\text{real } (\text{totient } n) = \text{real } n * (\prod_{p \in \text{prime-factors } n}. 1 - 1 / \text{real } p)$
 $\langle \text{proof} \rangle$

lemma *totient-gcd*: $\text{totient } (a * b) * \text{totient } (\text{gcd } a \ b) = \text{totient } a * \text{totient } b * \text{gcd } a \ b$
 $\langle \text{proof} \rangle$

lemma *totient-mult*: $\text{totient } (a * b) = \text{totient } a * \text{totient } b * \text{gcd } a \ b \ \text{div } \text{totient } (\text{gcd } a \ b)$
 $\langle \text{proof} \rangle$

lemma *of-nat-eq-1-iff*: $\text{of-nat } x = (1 :: 'a :: \{\text{semiring-1}, \text{semiring-char-0}\}) \longleftrightarrow x = 1$

$\langle \text{proof} \rangle$

lemma *odd-imp-coprime-nat*:

assumes *odd* (*n::nat*)

shows *coprime* *n* 2

$\langle \text{proof} \rangle$

lemma *totient-double*: *totient* ($2 * n$) = (if even *n* then $2 * \text{totient } n$ else *totient* *n*)

$\langle \text{proof} \rangle$

lemma *totient-power-Suc*: *totient* ($n \wedge \text{Suc } m$) = $n \wedge m * \text{totient } n$

$\langle \text{proof} \rangle$

lemma *totient-power*: $m > 0 \implies \text{totient } (n \wedge m) = n \wedge (m - 1) * \text{totient } n$

$\langle \text{proof} \rangle$

lemma *totient-gcd-lcm*: *totient* (*gcd* *a* *b*) * *totient* (*lcm* *a* *b*) = *totient* *a* * *totient* *b*

$\langle \text{proof} \rangle$

end

4 Residue rings

theory *Residues*

imports

Cong

HOL-Algebra.Multiplicative-Group

Totient

begin

definition *QuadRes* :: *int* $\Rightarrow$ *int* $\Rightarrow$ *bool*

where *QuadRes* *p* *a* = ($\exists y. ([y^2 = a] \text{ (mod } p))$)

definition *Legendre* :: *int* $\Rightarrow$ *int* $\Rightarrow$ *int*

where *Legendre* *a* *p* =

(if ($[a = 0] \text{ (mod } p)$) then 0

else if *QuadRes* *p* *a* then 1

else -1)

4.1 A locale for residue rings

definition *residue-ring* :: *int* $\Rightarrow$ *int* *ring*

where

residue-ring *m* =

(*carrier* = $\{0..m - 1\}$,

monoid.mult = $\lambda x y. (x * y) \text{ mod } m$,

one = 1,

```

    zero = 0,
    add = λx y. (x + y) mod m)

locale residues =
  fixes m :: int and R (structure)
  assumes m-gt-one: m > 1
  defines R ≡ residue-ring m
begin

lemma abelian-group: abelian-group R
  ⟨proof⟩

lemma comm-monoid: comm-monoid R
  ⟨proof⟩

lemma cring: cring R
  ⟨proof⟩

end

sublocale residues < cring
  ⟨proof⟩

context residues
begin

These lemmas translate back and forth between internal and external concepts.

lemma res-carrier-eq: carrier R = {0..m - 1}
  ⟨proof⟩

lemma res-add-eq: x ⊕ y = (x + y) mod m
  ⟨proof⟩

lemma res-mult-eq: x ⊗ y = (x * y) mod m
  ⟨proof⟩

lemma res-zero-eq: 0 = 0
  ⟨proof⟩

lemma res-one-eq: 1 = 1
  ⟨proof⟩

lemma res-units-eq: Units R = {x. 0 < x ∧ x < m ∧ coprime x m}
  ⟨proof⟩

lemma res-neg-eq: ⊖ x = (- x) mod m
  ⟨proof⟩

```

lemma *finite* [iff]: *finite* (*carrier* *R*)
 ⟨*proof*⟩

lemma *finite-Units* [iff]: *finite* (*Units* *R*)
 ⟨*proof*⟩

The function $a \mapsto a \bmod m$ maps the integers to the residue classes. The following lemmas show that this mapping respects addition and multiplication on the integers.

lemma *mod-in-carrier* [iff]: $a \bmod m \in \text{carrier } R$
 ⟨*proof*⟩

lemma *add-cong*: $(x \bmod m) \oplus (y \bmod m) = (x + y) \bmod m$
 ⟨*proof*⟩

lemma *mult-cong*: $(x \bmod m) \otimes (y \bmod m) = (x * y) \bmod m$
 ⟨*proof*⟩

lemma *zero-cong*: $0 = 0$
 ⟨*proof*⟩

lemma *one-cong*: $1 = 1 \bmod m$
 ⟨*proof*⟩

lemma *pow-cong*: $(x \bmod m) [\wedge] n = x^{\wedge n} \bmod m$
 ⟨*proof*⟩

lemma *neg-cong*: $\ominus (x \bmod m) = (- x) \bmod m$
 ⟨*proof*⟩

lemma (*in residues*) *prod-cong*: $\text{finite } A \implies (\bigotimes_{i \in A}. (f \ i) \bmod m) = (\prod_{i \in A}. f \ i) \bmod m$
 ⟨*proof*⟩

lemma (*in residues*) *sum-cong*: $\text{finite } A \implies (\bigoplus_{i \in A}. (f \ i) \bmod m) = (\sum_{i \in A}. f \ i) \bmod m$
 ⟨*proof*⟩

lemma *mod-in-res-units* [*simp*]:
 assumes $1 < m$ and *coprime* $a \ m$
 shows $a \bmod m \in \text{Units } R$
 ⟨*proof*⟩

lemma *res-eq-to-cong*: $(a \bmod m) = (b \bmod m) \longleftrightarrow [a = b] \ (mod \ m)$
 ⟨*proof*⟩

Simplifying with these will translate a ring equation in R to a congruence.

```

lemmas res-to-cong-simps =
  add-cong mult-cong pow-cong one-cong
  prod-cong sum-cong neg-cong res-eq-to-cong

```

Other useful facts about the residue ring.

```

lemma one-eq-neg-one:  $\mathbf{1} = \ominus \mathbf{1} \implies m = 2$ 
   $\langle \text{proof} \rangle$ 

```

end

4.2 Prime residues

```

locale residues-prime =
  fixes  $p :: \text{nat}$  and  $R$  (structure)
  assumes  $p\text{-prime}$  [intro]:  $\text{prime } p$ 
  defines  $R \equiv \text{residue-ring } (\text{int } p)$ 

```

```

sublocale residues-prime < residues  $p$ 
   $\langle \text{proof} \rangle$ 

```

```

context residues-prime
begin

```

```

lemma p-coprime-left:
   $\text{coprime } p \ a \iff \neg p \ \text{dvd } a$ 
   $\langle \text{proof} \rangle$ 

```

```

lemma p-coprime-right:
   $\text{coprime } a \ p \iff \neg p \ \text{dvd } a$ 
   $\langle \text{proof} \rangle$ 

```

```

lemma p-coprime-left-int:
   $\text{coprime } (\text{int } p) \ a \iff \neg \text{int } p \ \text{dvd } a$ 
   $\langle \text{proof} \rangle$ 

```

```

lemma p-coprime-right-int:
   $\text{coprime } a \ (\text{int } p) \iff \neg \text{int } p \ \text{dvd } a$ 
   $\langle \text{proof} \rangle$ 

```

```

lemma is-field:  $\text{field } R$ 
   $\langle \text{proof} \rangle$ 

```

```

lemma res-prime-units-eq:  $\text{Units } R = \{1..p - 1\}$ 
   $\langle \text{proof} \rangle$ 

```

end

```

sublocale residues-prime < field
   $\langle \text{proof} \rangle$ 

```

5 Test cases: Euler's theorem and Wilson's theorem

5.1 Euler's theorem

lemma (in *residues*) *totatives-eq*:
 $\text{totatives } (\text{nat } m) = \text{nat } \text{Units } R$
 <proof>

lemma (in *residues*) *totient-eq*:
 $\text{totient } (\text{nat } m) = \text{card } (\text{Units } R)$
 <proof>

lemma (in *residues-prime*) *totient-eq*: $\text{totient } p = p - 1$
 <proof>

lemma (in *residues*) *euler-theorem*:
 assumes *coprime* $a\ m$
 shows $[a \wedge \text{totient } (\text{nat } m) = 1] \pmod m$
 <proof>

lemma *euler-theorem*:
 fixes $a\ m :: \text{nat}$
 assumes *coprime* $a\ m$
 shows $[a \wedge \text{totient } m = 1] \pmod m$
 <proof>

lemma *fermat-theorem*:
 fixes $p\ a :: \text{nat}$
 assumes *prime* p and $\neg p \text{ dvd } a$
 shows $[a \wedge (p - 1) = 1] \pmod p$
 <proof>

5.2 Wilson's theorem

lemma (in *field*) *inv-pair-lemma*: $x \in \text{Units } R \implies y \in \text{Units } R \implies$
 $\{x, \text{inv } x\} \neq \{y, \text{inv } y\} \implies \{x, \text{inv } x\} \cap \{y, \text{inv } y\} = \{\}$
 <proof>

lemma (in *residues-prime*) *wilson-theorem1*:
 assumes $a: p > 2$
 shows $[\text{fact } (p - 1) = (-1::\text{int})] \pmod p$
 <proof>

lemma *wilson-theorem*:
 assumes *prime* p
 shows $[\text{fact } (p - 1) = -1] \pmod p$
 <proof>

This result can be transferred to the multiplicative group of $\mathbb{Z}/p\mathbb{Z}$ for p

prime.

lemma *mod-nat-int-pow-eq*:

fixes $n :: \text{nat}$ **and** $p \ a :: \text{int}$

shows $a \geq 0 \implies p \geq 0 \implies (\text{nat } a \wedge n) \bmod (\text{nat } p) = \text{nat } ((a \wedge n) \bmod p)$

<proof>

theorem *residue-prime-mult-group-has-gen*:

fixes $p :: \text{nat}$

assumes *prime-p* : *prime p*

shows $\exists a \in \{1 \dots p - 1\}. \{1 \dots p - 1\} = \{a^i \bmod p \mid i \in \text{UNIV}\}$

<proof>

5.3 Upper bound for the number of n -th roots

lemma *roots-mod-prime-bound*:

fixes $n \ c \ p :: \text{nat}$

assumes *prime p* $n > 0$

defines $A \equiv \{x \in \{..<p\}. [x \wedge n = c] \bmod p\}$

shows $\text{card } A \leq n$

<proof>

end

6 The sieve of Eratosthenes

theory *Eratosthenes*

imports *Main HOL-Computational-Algebra.Primes*

begin

6.1 Preliminary: strict divisibility

context *dvd*

begin

abbreviation *dvd-strict* :: $'a \Rightarrow 'a \Rightarrow \text{bool}$ (**infixl** *dvd'-strict* 50)

where

$b \text{ dvd-strict } a \equiv b \text{ dvd } a \wedge \neg a \text{ dvd } b$

end

6.2 Main corpus

The sieve is modelled as a list of booleans, where *False* means *marked out*.

type-synonym *marks* = *bool list*

definition *numbers-of-marks* :: $\text{nat} \Rightarrow \text{marks} \Rightarrow \text{nat set}$

where

$numbers-of-marks\ n\ bs = fst\ ' \{x \in set\ (enumerate\ n\ bs).\ snd\ x\}$

lemma *numbers-of-marks-simps* [simp, code]:

$numbers-of-marks\ n\ [] = \{\}$
 $numbers-of-marks\ n\ (True\ \#\ bs) = insert\ n\ (numbers-of-marks\ (Suc\ n)\ bs)$
 $numbers-of-marks\ n\ (False\ \#\ bs) = numbers-of-marks\ (Suc\ n)\ bs$
 $\langle proof \rangle$

lemma *numbers-of-marks-Suc*:

$numbers-of-marks\ (Suc\ n)\ bs = Suc\ ' \ numbers-of-marks\ n\ bs$
 $\langle proof \rangle$

lemma *numbers-of-marks-replicate-False* [simp]:

$numbers-of-marks\ n\ (replicate\ m\ False) = \{\}$
 $\langle proof \rangle$

lemma *numbers-of-marks-replicate-True* [simp]:

$numbers-of-marks\ n\ (replicate\ m\ True) = \{n..<n+m\}$
 $\langle proof \rangle$

lemma *in-numbers-of-marks-eq*:

$m \in numbers-of-marks\ n\ bs \longleftrightarrow m \in \{n..<n + length\ bs\} \wedge bs\ !\ (m - n)$
 $\langle proof \rangle$

lemma *sorted-list-of-set-numbers-of-marks*:

$sorted-list-of-set\ (numbers-of-marks\ n\ bs) = map\ fst\ (filter\ snd\ (enumerate\ n\ bs))$
 $\langle proof \rangle$

Marking out multiples in a sieve

definition *mark-out* :: $nat \Rightarrow marks \Rightarrow marks$

where

$mark-out\ n\ bs = map\ (\lambda(q, b). b \wedge \neg Suc\ n\ dvd\ Suc\ (Suc\ q))\ (enumerate\ n\ bs)$

lemma *mark-out-Nil* [simp]: $mark-out\ n\ [] = []$

$\langle proof \rangle$

lemma *length-mark-out* [simp]: $length\ (mark-out\ n\ bs) = length\ bs$

$\langle proof \rangle$

lemma *numbers-of-marks-mark-out*:

$numbers-of-marks\ n\ (mark-out\ m\ bs) = \{q \in numbers-of-marks\ n\ bs. \neg Suc\ m\ dvd\ Suc\ q - n\}$
 $\langle proof \rangle$

Auxiliary operation for efficient implementation

definition *mark-out-aux* :: $nat \Rightarrow nat \Rightarrow marks \Rightarrow marks$

where

$mark-out-aux\ n\ m\ bs =$
 $map\ (\lambda(q, b). b \wedge (q < m + n \vee \neg Suc\ n\ dvd\ Suc\ (Suc\ q) + (n - m\ mod\ Suc$

$n)))$ (*enumerate* n bs)

lemma *mark-out-code* [*code*]: *mark-out* n bs = *mark-out-aux* n n bs
 <proof>

lemma *mark-out-aux-simps* [*simp*, *code*]:
mark-out-aux n m [] = []
mark-out-aux n 0 ($b \# bs$) = *False* # *mark-out-aux* n n bs
mark-out-aux n (*Suc* m) ($b \# bs$) = $b \#$ *mark-out-aux* n m bs
 <proof>

Main entry point to sieve

fun *sieve* :: *nat* $\Rightarrow$ *marks* $\Rightarrow$ *marks*
where
sieve n [] = []
| *sieve* n (*False* # bs) = *False* # *sieve* (*Suc* n) bs
| *sieve* n (*True* # bs) = *True* # *sieve* (*Suc* n) (*mark-out* n bs)

There are the following possible optimisations here:

- *sieve* can abort as soon as n is too big to let *mark-out* have any effect.
- Search for further primes can be given up as soon as the search position exceeds the square root of the maximum candidate.

This is left as an constructive exercise to the reader.

lemma *numbers-of-marks-sieve*:
numbers-of-marks (*Suc* n) (*sieve* n bs) =
 $\{q \in \text{numbers-of-marks } (\text{Suc } n) \text{ } bs. \forall m \in \text{numbers-of-marks } (\text{Suc } n) \text{ } bs. \neg m \text{ dvd-strict } q\}$
 <proof>

Relation of the sieve algorithm to actual primes

definition *primes-upto* :: *nat* $\Rightarrow$ *nat list*
where
primes-upto n = *sorted-list-of-set* $\{m. m \leq n \wedge \text{prime } m\}$

lemma *set-primes-upto*: *set* (*primes-upto* n) = $\{m. m \leq n \wedge \text{prime } m\}$
 <proof>

lemma *sorted-primes-upto* [*iff*]: *sorted* (*primes-upto* n)
 <proof>

lemma *distinct-primes-upto* [*iff*]: *distinct* (*primes-upto* n)
 <proof>

lemma *set-primes-upto-sieve*:
set (*primes-upto* n) = *numbers-of-marks* 2 (*sieve* 1 (*replicate* ($n - 1$) *True*))

<proof>

lemma *primes-upto-sieve* [code]:

primes-upto n = map fst (filter snd (enumerate 2 (sieve 1 (replicate (n - 1) True))))

<proof>

lemma *prime-in-primes-upto*: *prime n $\longleftrightarrow$ n $\in$ set (primes-upto n)*

<proof>

6.3 Application: smallest prime beyond a certain number

definition *smallest-prime-beyond* :: *nat $\Rightarrow$ nat*

where

smallest-prime-beyond n = (LEAST p. prime p $\wedge$ p $\geq$ n)

lemma *prime-smallest-prime-beyond* [iff]: *prime (smallest-prime-beyond n) (is ?P)*

and *smallest-prime-beyond-le* [iff]: *smallest-prime-beyond n $\geq$ n (is ?Q)*

<proof>

lemma *smallest-prime-beyond-smallest*: *prime p $\implies$ p $\geq$ n $\implies$ smallest-prime-beyond*

n $\leq$ p

<proof>

lemma *smallest-prime-beyond-eq*:

prime p $\implies$ p $\geq$ n $\implies$ ($\bigwedge q$. prime q $\implies$ q $\geq$ n $\implies$ q $\geq$ p) $\implies$ smallest-prime-beyond n = p

<proof>

definition *smallest-prime-between* :: *nat $\Rightarrow$ nat $\Rightarrow$ nat option*

where

smallest-prime-between m n =

(if ($\exists p$. prime p $\wedge$ m $\leq$ p $\wedge$ p $\leq$ n) then Some (smallest-prime-beyond m) else None)

lemma *smallest-prime-between-None*:

smallest-prime-between m n = None $\longleftrightarrow$ ($\forall q$. m $\leq$ q $\wedge$ q $\leq$ n $\longrightarrow$ $\neg$ prime q)

<proof>

lemma *smallest-prime-between-Some*:

smallest-prime-between m n = Some p $\longleftrightarrow$ smallest-prime-beyond m = p $\wedge$ p $\leq$ n

<proof>

lemma [code]: *smallest-prime-between m n = List.find (λp . p $\geq$ m) (primes-upto n)*

<proof>

definition *smallest-prime-beyond-aux* :: *nat* $\Rightarrow$ *nat* $\Rightarrow$ *nat*
where
smallest-prime-beyond-aux *k n* = *smallest-prime-beyond* *n*

lemma [code]:
smallest-prime-beyond-aux *k n* =
 (case *smallest-prime-between* *n* (*k* * *n*) of
 Some *p* $\Rightarrow$ *p*
 | None $\Rightarrow$ *smallest-prime-beyond-aux* (*Suc* *k*) *n*)
 <proof>

lemma [code]: *smallest-prime-beyond* *n* = *smallest-prime-beyond-aux* 2 *n*
 <proof>

end

7 Fast modular exponentiation

theory *Mod-Exp*
imports *Cong HOL-Library.Power-By-Squaring*
begin

context *euclidean-semiring-cancel*
begin

definition *mod-exp-aux* :: '*a* $\Rightarrow$ '*a* $\Rightarrow$ '*a* $\Rightarrow$ *nat* $\Rightarrow$ '*a*
where *mod-exp-aux* *m* = *efficient-funpow* ($\lambda x y. x * y \bmod m$)

lemma *mod-exp-aux-code* [code]:
mod-exp-aux *m y x n* =
 (if *n* = 0 then *y*
 else if *n* = 1 then (*x* * *y*) mod *m*
 else if even *n* then *mod-exp-aux* *m y* ((*x* * *x*) mod *m*) (*n* div 2)
 else *mod-exp-aux* *m* ((*x* * *y*) mod *m*) ((*x* * *x*) mod *m*) (*n* div 2))
 <proof>

lemma *mod-exp-aux-correct*:
mod-exp-aux *m y x n* mod *m* = (*x* $\wedge^n$ * *y*) mod *m*
 <proof>

definition *mod-exp* :: '*a* $\Rightarrow$ *nat* $\Rightarrow$ '*a* $\Rightarrow$ '*a*
where *mod-exp* *b e m* = (*b* $\wedge^e$) mod *m*

lemma *mod-exp-code* [code]: *mod-exp* *b e m* = *mod-exp-aux* *m 1 b e* mod *m*
 <proof>

end

lemmas $[code-abbrev] = mod-exp-def[where \text{ ?'a} = nat] \ mod-exp-def[where \text{ ?'a} = int]$

lemma *cong-power-nat-code* $[code-unfold]$:
 $[b \wedge e = (x :: nat)] \ (mod \ m) \longleftrightarrow mod-exp \ b \ e \ m = x \ mod \ m$
 $\langle proof \rangle$

lemma *cong-power-int-code* $[code-unfold]$:
 $[b \wedge e = (x :: int)] \ (mod \ m) \longleftrightarrow mod-exp \ b \ e \ m = x \ mod \ m$
 $\langle proof \rangle$

The following rules allow the simplifier to evaluate *mod-exp* efficiently.

lemma *eval-mod-exp-aux* $[simp]$:
 $mod-exp-aux \ m \ y \ x \ 0 = y$
 $mod-exp-aux \ m \ y \ x \ (Suc \ 0) = (x * y) \ mod \ m$
 $mod-exp-aux \ m \ y \ x \ (numeral \ (num.Bit0 \ n)) =$
 $\quad mod-exp-aux \ m \ y \ (x^2 \ mod \ m) \ (numeral \ n)$
 $mod-exp-aux \ m \ y \ x \ (numeral \ (num.Bit1 \ n)) =$
 $\quad mod-exp-aux \ m \ ((x * y) \ mod \ m) \ (x^2 \ mod \ m) \ (numeral \ n)$
 $\langle proof \rangle$

lemma *eval-mod-exp* $[simp]$:
 $mod-exp \ b' \ 0 \ m' = 1 \ mod \ m'$
 $mod-exp \ b' \ 1 \ m' = b' \ mod \ m'$
 $mod-exp \ b' \ (Suc \ 0) \ m' = b' \ mod \ m'$
 $mod-exp \ b' \ e' \ 0 = b' \wedge e'$
 $mod-exp \ b' \ e' \ 1 = 0$
 $mod-exp \ b' \ e' \ (Suc \ 0) = 0$
 $mod-exp \ 0 \ 1 \ m' = 0$
 $mod-exp \ 0 \ (Suc \ 0) \ m' = 0$
 $mod-exp \ 0 \ (numeral \ e) \ m' = 0$
 $mod-exp \ 1 \ e' \ m' = 1 \ mod \ m'$
 $mod-exp \ (Suc \ 0) \ e' \ m' = 1 \ mod \ m'$
 $mod-exp \ (numeral \ b) \ (numeral \ e) \ (numeral \ m) =$
 $\quad mod-exp-aux \ (numeral \ m) \ 1 \ (numeral \ b) \ (numeral \ e) \ mod \ numeral \ m$
 $\langle proof \rangle$

end

theory *Euler-Criterion*
imports *Residues*
begin

context
fixes $p :: nat$
fixes $a :: int$

assumes $p\text{-prime}: prime \ p$

```

assumes p-ge-2:  $2 < p$ 
assumes p-a-relprime:  $[a \neq 0](\text{mod } p)$ 
begin

private lemma odd-p: odd p
  <proof> lemma p-minus-1-int:
    int  $(p - 1) = \text{int } p - 1$ 
  <proof> lemma p-not-eq-Suc-0 [simp]:
     $p \neq \text{Suc } 0$ 
  <proof> lemma one-mod-int-p-eq [simp]:
     $1 \text{ mod int } p = 1$ 
<proof> lemma E-1:
  assumes QuadRes  $(\text{int } p) \ a$ 
  shows  $[a \wedge ((p - 1) \text{ div } 2) = 1] (\text{mod int } p)$ 
<proof> definition S1 :: int set where  $S1 = \{0 <.. \text{int } p - 1\}$ 

private definition P :: int  $\Rightarrow$  int  $\Rightarrow$  bool where
   $P \ x \ y \longleftrightarrow [x * y = a] (\text{mod } p) \wedge y \in S1$ 

private definition f-1 :: int  $\Rightarrow$  int where
   $f-1 \ x = (\text{THE } y. P \ x \ y)$ 

private definition f :: int  $\Rightarrow$  int set where
   $f \ x = \{x, f-1 \ x\}$ 

private definition S2 :: int set set where  $S2 = f \ ` \ S1$ 

private lemma P-lemma: assumes  $x \in S1$ 
  shows  $\exists! y. P \ x \ y$ 
<proof> lemma f-1-lemma-1: assumes  $x \in S1$ 
  shows  $P \ x \ (f-1 \ x)$  <proof> lemma f-1-lemma-2: assumes  $x \in S1$ 
  shows  $f-1 \ (f-1 \ x) = x$ 
<proof> lemma f-lemma-1: assumes  $x \in S1$ 
  shows  $f \ x = f \ (f-1 \ x)$  <proof> lemma l1: assumes  $\neg \text{QuadRes } p \ a \ x \in S1$ 
  shows  $x \neq f-1 \ x$ 
<proof> lemma l2: assumes  $\neg \text{QuadRes } p \ a \ x \in S1$ 
  shows  $\prod (f \ x) = a] (\text{mod } p)$ 
<proof> lemma l3: assumes  $x \in S2$ 
  shows finite  $x$  <proof> lemma l4:  $S1 = \bigcup S2$  <proof> lemma l5: assumes  $x$ 
 $\in S2 \ y \in S2 \ x \neq y$ 
  shows  $x \cap y = \{\}$ 
<proof> lemma l6:  $\text{prod Prod } S2 = \prod S1$ 
  <proof> lemma l7:  $\text{fact } n = \prod \{0 <.. \text{int } n\}$ 
<proof> lemma l8:  $\text{fact } (p - 1) = \prod S1$  <proof> lemma l9:  $[\text{prod Prod } S2 = -1]$ 
 $(\text{mod } p)$ 
<proof> lemma l10: assumes  $\text{card } S = n \wedge x. x \in S \implies [g \ x = a] (\text{mod } p)$ 
  shows  $[\text{prod } g \ S = a \wedge n] (\text{mod } p)$  <proof> lemma l11: assumes  $\neg \text{QuadRes } p \ a$ 
  shows  $\text{card } S2 = (p - 1) \text{ div } 2$ 
<proof> lemma l12: assumes  $\neg \text{QuadRes } p \ a$ 

```

```

  shows [prod Prod S2 = a ^ ((p - 1) div 2)] (mod p)
  <proof> lemma E-2: assumes ¬ QuadRes p a
  shows [a ^ ((p - 1) div 2) = -1] (mod p) <proof>

lemma euler-criterion-aux: [(Legendre a p) = a ^ ((p - 1) div 2)] (mod p)
  <proof>

end

theorem euler-criterion: assumes prime p 2 < p
  shows [(Legendre a p) = a ^ ((p - 1) div 2)] (mod p)
  <proof>

hide-fact euler-criterion-aux

end

```

8 Gauss' Lemma

```

theory Gauss
  imports Euler-Criterion
begin

lemma cong-prime-prod-zero-nat:
  [a * b = 0] (mod p) ⇒ prime p ⇒ [a = 0] (mod p) ∨ [b = 0] (mod p)
  for a :: nat
  <proof>

lemma cong-prime-prod-zero-int:
  [a * b = 0] (mod p) ⇒ prime p ⇒ [a = 0] (mod p) ∨ [b = 0] (mod p)
  for a :: int
  <proof>

locale GAUSS =
  fixes p :: nat
  fixes a :: int
  assumes p-prime: prime p
  assumes p-ge-2: 2 < p
  assumes p-a-relprime: [a ≠ 0] (mod p)
  assumes a-nonzero: 0 < a
begin

definition A = {0::int <.. ((int p - 1) div 2)}
definition B = (λx. x * a) ' A
definition C = (λx. x mod p) ' B
definition D = C ∩ {.. (int p - 1) div 2}
definition E = C ∩ {(int p - 1) div 2 <..}
definition F = (λx. (int p - x)) ' E

```

8.1 Basic properties of p

lemma *odd-p*: *odd p*
⟨*proof*⟩

lemma *p-minus-one-l*: $(\text{int } p - 1) \text{ div } 2 < p$
⟨*proof*⟩

lemma *p-eq2*: $\text{int } p = (2 * ((\text{int } p - 1) \text{ div } 2)) + 1$
⟨*proof*⟩

lemma *p-odd-int*: **obtains** $z :: \text{int}$ **where** $\text{int } p = 2 * z + 1$ $0 < z$
⟨*proof*⟩

8.2 Basic Properties of the Gauss Sets

lemma *finite-A*: *finite A*
⟨*proof*⟩

lemma *finite-B*: *finite B*
⟨*proof*⟩

lemma *finite-C*: *finite C*
⟨*proof*⟩

lemma *finite-D*: *finite D*
⟨*proof*⟩

lemma *finite-E*: *finite E*
⟨*proof*⟩

lemma *finite-F*: *finite F*
⟨*proof*⟩

lemma *C-eq*: $C = D \cup E$
⟨*proof*⟩

lemma *A-card-eq*: $\text{card } A = \text{nat } ((\text{int } p - 1) \text{ div } 2)$
⟨*proof*⟩

lemma *inj-on-xa-A*: *inj-on* $(\lambda x. x * a)$ *A*
⟨*proof*⟩

definition *ResSet* :: $\text{int} \Rightarrow \text{int set} \Rightarrow \text{bool}$
where $\text{ResSet } m \ X \longleftrightarrow (\forall y1 \ y2. y1 \in X \wedge y2 \in X \wedge [y1 = y2] \ (\text{mod } m) \longrightarrow y1 = y2)$

lemma *ResSet-image*:
 $0 < m \Longrightarrow \text{ResSet } m \ A \Longrightarrow \forall x \in A. \forall y \in A. ([f \ x = f \ y] \ (\text{mod } m) \longrightarrow x = y) \Longrightarrow \text{ResSet } m \ (f \ ` \ A)$

$\langle \text{proof} \rangle$

lemma *A-res*: $\text{ResSet } p \ A$
 $\langle \text{proof} \rangle$

lemma *B-res*: $\text{ResSet } p \ B$
 $\langle \text{proof} \rangle$

lemma *SR-B-inj*: $\text{inj-on } (\lambda x. x \bmod p) \ B$
 $\langle \text{proof} \rangle$

lemma *inj-on-pminus-E*: $\text{inj-on } (\lambda x. p - x) \ E$
 $\langle \text{proof} \rangle$

lemma *nonzero-mod-p*: $0 < x \implies x < \text{int } p \implies [x \neq 0](\text{mod } p)$
for $x :: \text{int}$
 $\langle \text{proof} \rangle$

lemma *A-ncong-p*: $x \in A \implies [x \neq 0](\text{mod } p)$
 $\langle \text{proof} \rangle$

lemma *A-greater-zero*: $x \in A \implies 0 < x$
 $\langle \text{proof} \rangle$

lemma *B-ncong-p*: $x \in B \implies [x \neq 0](\text{mod } p)$
 $\langle \text{proof} \rangle$

lemma *B-greater-zero*: $x \in B \implies 0 < x$
 $\langle \text{proof} \rangle$

lemma *B-mod-greater-zero*:
 $0 < x \bmod \text{int } p$ **if** $x \in B$
 $\langle \text{proof} \rangle$

lemma *C-greater-zero*: $y \in C \implies 0 < y$
 $\langle \text{proof} \rangle$

lemma *F-subset*: $F \subseteq \{x. 0 < x \wedge x \leq ((\text{int } p - 1) \text{ div } 2)\}$
 $\langle \text{proof} \rangle$

lemma *D-subset*: $D \subseteq \{x. 0 < x \wedge x \leq ((p - 1) \text{ div } 2)\}$
 $\langle \text{proof} \rangle$

lemma *F-eq*: $F = \{x. \exists y \in A. (x = p - ((y * a) \bmod p) \wedge (\text{int } p - 1) \text{ div } 2 < (y * a) \bmod p)\}$
 $\langle \text{proof} \rangle$

lemma *D-eq*: $D = \{x. \exists y \in A. (x = (y * a) \bmod p \wedge (y * a) \bmod p \leq (\text{int } p - 1) \text{ div } 2)\}$

$\langle \text{proof} \rangle$

lemma *all-A-relprime:*
coprime x p if $x \in A$
 $\langle \text{proof} \rangle$

lemma *A-prod-relprime:* *coprime (prod id A) p*
 $\langle \text{proof} \rangle$

8.3 Relationships Between Gauss Sets

lemma *StandardRes-inj-on-ResSet:* *ResSet m X $\implies$ inj-on ($\lambda b. b \bmod m$) X*
 $\langle \text{proof} \rangle$

lemma *B-card-eq-A:* *card B = card A*
 $\langle \text{proof} \rangle$

lemma *B-card-eq:* *card B = nat ((int p - 1) div 2)*
 $\langle \text{proof} \rangle$

lemma *F-card-eq-E:* *card F = card E*
 $\langle \text{proof} \rangle$

lemma *C-card-eq-B:* *card C = card B*
 $\langle \text{proof} \rangle$

lemma *D-E-disj:* *$D \cap E = \{\}$*
 $\langle \text{proof} \rangle$

lemma *C-card-eq-D-plus-E:* *card C = card D + card E*
 $\langle \text{proof} \rangle$

lemma *C-prod-eq-D-times-E:* *prod id E * prod id D = prod id C*
 $\langle \text{proof} \rangle$

lemma *C-B-zcong-prod:* *[prod id C = prod id B] (mod p)*
 $\langle \text{proof} \rangle$

lemma *F-Un-D-subset:* *$(F \cup D) \subseteq A$*
 $\langle \text{proof} \rangle$

lemma *F-D-disj:* *$(F \cap D) = \{\}$*
 $\langle \text{proof} \rangle$

lemma *F-Un-D-card:* *card (F $\cup$ D) = nat ((p - 1) div 2)*
 $\langle \text{proof} \rangle$

lemma *F-Un-D-eq-A:* *F $\cup$ D = A*
 $\langle \text{proof} \rangle$

lemma *prod-D-F-eq-prod-A*: $\text{prod id } D * \text{prod id } F = \text{prod id } A$
 $\langle \text{proof} \rangle$

lemma *prod-F-zcong*: $[\text{prod id } F = ((-1)^\wedge(\text{card } E)) * \text{prod id } E] \pmod{p}$
 $\langle \text{proof} \rangle$

8.4 Gauss' Lemma

lemma *aux*: $\text{prod id } A * (-1)^\wedge \text{card } E * a^\wedge \text{card } A * (-1)^\wedge \text{card } E = \text{prod id } A * a^\wedge \text{card } A$
 $\langle \text{proof} \rangle$

theorem *pre-gauss-lemma*: $[a^\wedge \text{nat}((\text{int } p - 1) \text{ div } 2) = (-1)^\wedge(\text{card } E)] \pmod{p}$
 $\langle \text{proof} \rangle$

theorem *gauss-lemma*: *Legendre* $a \text{ p} = (-1)^\wedge(\text{card } E)$
 $\langle \text{proof} \rangle$

end

end

theory *Quadratic-Reciprocity*
imports *Gauss*
begin

The proof is based on Gauss's fifth proof, which can be found at <https://www.lehigh.edu/~shw2/q-ecip/gauss5.pdf>.

locale *QR* =
fixes $p :: \text{nat}$
fixes $q :: \text{nat}$
assumes $p\text{-prime}$: *prime* p
assumes $p\text{-ge-2}$: $2 < p$
assumes $q\text{-prime}$: *prime* q
assumes $q\text{-ge-2}$: $2 < q$
assumes $pq\text{-neq}$: $p \neq q$
begin

lemma *odd-p*: *odd* p
 $\langle \text{proof} \rangle$

lemma *p-ge-0*: $0 < \text{int } p$
 $\langle \text{proof} \rangle$

lemma *p-eq2*: $\text{int } p = (2 * ((\text{int } p - 1) \text{ div } 2)) + 1$
 $\langle \text{proof} \rangle$

lemma *odd-q*: *odd q*

<proof>

lemma *q-ge-0*: $0 < \text{int } q$

<proof>

lemma *q-eq2*: $\text{int } q = (2 * ((\text{int } q - 1) \text{ div } 2)) + 1$

<proof>

lemma *pq-eq2*: $\text{int } p * \text{int } q = (2 * ((\text{int } p * \text{int } q - 1) \text{ div } 2)) + 1$

<proof>

lemma *pq-coprime*: *coprime p q*

<proof>

lemma *pq-coprime-int*: *coprime (int p) (int q)*

<proof>

lemma *qp-ineq*: $\text{int } p * k \leq (\text{int } p * \text{int } q - 1) \text{ div } 2 \longleftrightarrow k \leq (\text{int } q - 1) \text{ div } 2$

<proof>

lemma *QRqp*: *QR q p*

<proof>

lemma *pq-commute*: $\text{int } p * \text{int } q = \text{int } q * \text{int } p$

<proof>

lemma *pq-ge-0*: $\text{int } p * \text{int } q > 0$

<proof>

definition $r = ((p - 1) \text{ div } 2) * ((q - 1) \text{ div } 2)$

definition $m = \text{card } (\text{GAUSS}.E \text{ } p \text{ } q)$

definition $n = \text{card } (\text{GAUSS}.E \text{ } q \text{ } p)$

abbreviation $\text{Res } k \equiv \{0 .. k - 1\} \text{ for } k :: \text{int}$

abbreviation $\text{Res-ge-0 } k \equiv \{0 <.. k - 1\} \text{ for } k :: \text{int}$

abbreviation $\text{Res-0 } k \equiv \{0 :: \text{int}\} \text{ for } k :: \text{int}$

abbreviation $\text{Res-l } k \equiv \{0 <.. (k - 1) \text{ div } 2\} \text{ for } k :: \text{int}$

abbreviation $\text{Res-h } k \equiv \{(k - 1) \text{ div } 2 <.. k - 1\} \text{ for } k :: \text{int}$

abbreviation $\text{Sets-pq } r0 \text{ } r1 \text{ } r2 \equiv$

$\{(x :: \text{int}). x \in r0 \text{ } (\text{int } p * \text{int } q) \wedge x \bmod p \in r1 \text{ } (\text{int } p) \wedge x \bmod q \in r2 \text{ } (\text{int } q)\}$

definition $A = \text{Sets-pq } \text{Res-l } \text{Res-l } \text{Res-h}$

definition $B = \text{Sets-pq } \text{Res-l } \text{Res-h } \text{Res-l}$

definition $C = \text{Sets-pq } \text{Res-h } \text{Res-h } \text{Res-l}$

definition $D = \text{Sets-pq } \text{Res-l } \text{Res-h } \text{Res-h}$

definition $E = \text{Sets-pq } \text{Res-l } \text{Res-0 } \text{Res-h}$

definition $F = \text{Sets-pq Res-l Res-h Res-0}$

definition $a = \text{card } A$

definition $b = \text{card } B$

definition $c = \text{card } C$

definition $d = \text{card } D$

definition $e = \text{card } E$

definition $f = \text{card } F$

lemma Gpq : $\text{GAUSS } p \ q$
 $\langle \text{proof} \rangle$

lemma Gqp : $\text{GAUSS } q \ p$
 $\langle \text{proof} \rangle$

lemma $QR\text{-lemma-01}$: $(\lambda x. x \bmod q) \text{ ' } E = \text{GAUSS.E } q \ p$
 $\langle \text{proof} \rangle$

lemma $QR\text{-lemma-02}$: $e = n$
 $\langle \text{proof} \rangle$

lemma $QR\text{-lemma-03}$: $f = m$
 $\langle \text{proof} \rangle$

definition $f\text{-1} :: \text{int} \Rightarrow \text{int} \times \text{int}$
where $f\text{-1 } x = ((x \bmod p), (x \bmod q))$

definition $P\text{-1} :: \text{int} \times \text{int} \Rightarrow \text{int} \Rightarrow \text{bool}$
where $P\text{-1 } \text{res } x \longleftrightarrow x \bmod p = \text{fst } \text{res} \wedge x \bmod q = \text{snd } \text{res} \wedge x \in \text{Res } (\text{int } p * \text{int } q)$

definition $g\text{-1} :: \text{int} \times \text{int} \Rightarrow \text{int}$
where $g\text{-1 } \text{res} = (\text{THE } x. P\text{-1 } \text{res } x)$

lemma $P\text{-1-lemma}$:
fixes $\text{res} :: \text{int} \times \text{int}$
assumes $0 \leq \text{fst } \text{res} \ \text{fst } \text{res} < p \ 0 \leq \text{snd } \text{res} \ \text{snd } \text{res} < q$
shows $\exists! x. P\text{-1 } \text{res } x$
 $\langle \text{proof} \rangle$

lemma $g\text{-1-lemma}$:
fixes $\text{res} :: \text{int} \times \text{int}$
assumes $0 \leq \text{fst } \text{res} \ \text{fst } \text{res} < p \ 0 \leq \text{snd } \text{res} \ \text{snd } \text{res} < q$
shows $P\text{-1 } \text{res} (g\text{-1 } \text{res})$
 $\langle \text{proof} \rangle$

definition $\text{BuC} = \text{Sets-pq Res-ge-0 Res-h Res-l}$

lemma finite-BuC $[\text{simp}]$:

finite BuC
 $\langle \text{proof} \rangle$

lemma *QR-lemma-04*: $\text{card BuC} = \text{card (Res-h } p \times \text{Res-l } q)$
 $\langle \text{proof} \rangle$

lemma *QR-lemma-05*: $\text{card (Res-h } p \times \text{Res-l } q) = r$
 $\langle \text{proof} \rangle$

lemma *QR-lemma-06*: $b + c = r$
 $\langle \text{proof} \rangle$

definition *f-2*:: $\text{int} \Rightarrow \text{int}$
 where $f-2 \ x = (\text{int } p * \text{int } q) - x$

lemma *f-2-lemma-1*: $f-2 \ (f-2 \ x) = x$
 $\langle \text{proof} \rangle$

lemma *f-2-lemma-2*: $[f-2 \ x = \text{int } p - x] \ (\text{mod } p)$
 $\langle \text{proof} \rangle$

lemma *f-2-lemma-3*: $f-2 \ x \in S \Longrightarrow x \in f-2 \ ' S$
 $\langle \text{proof} \rangle$

lemma *QR-lemma-07*:
 $f-2 \ ' \text{Res-l } (\text{int } p * \text{int } q) = \text{Res-h } (\text{int } p * \text{int } q)$
 $f-2 \ ' \text{Res-h } (\text{int } p * \text{int } q) = \text{Res-l } (\text{int } p * \text{int } q)$
 $\langle \text{proof} \rangle$

lemma *QR-lemma-08*:
 $f-2 \ x \text{ mod } p \in \text{Res-l } p \longleftrightarrow x \text{ mod } p \in \text{Res-h } p$
 $f-2 \ x \text{ mod } p \in \text{Res-h } p \longleftrightarrow x \text{ mod } p \in \text{Res-l } p$
 $\langle \text{proof} \rangle$

lemma *QR-lemma-09*:
 $f-2 \ x \text{ mod } q \in \text{Res-l } q \longleftrightarrow x \text{ mod } q \in \text{Res-h } q$
 $f-2 \ x \text{ mod } q \in \text{Res-h } q \longleftrightarrow x \text{ mod } q \in \text{Res-l } q$
 $\langle \text{proof} \rangle$

lemma *QR-lemma-10*: $a = c$
 $\langle \text{proof} \rangle$

definition *BuD* = *Sets-pq Res-l Res-h Res-ge-0*

definition *BuDUF* = *Sets-pq Res-l Res-h Res*

definition *f-3* :: $\text{int} \Rightarrow \text{int} \times \text{int}$
 where $f-3 \ x = (x \text{ mod } p, x \text{ div } p + 1)$

definition *g-3* :: $\text{int} \times \text{int} \Rightarrow \text{int}$

where $g\text{-}\mathcal{J} \ x = \text{fst } x + (\text{snd } x - 1) * p$

lemma *QR-lemma-11*: $\text{card } \text{BuDuF} = \text{card } (\text{Res-h } p \times \text{Res-l } q)$
 $\langle \text{proof} \rangle$

lemma *QR-lemma-12*: $b + d + m = r$
 $\langle \text{proof} \rangle$

lemma *QR-lemma-13*: $a + d + n = r$
 $\langle \text{proof} \rangle$

lemma *QR-lemma-14*: $(-1::\text{int}) \wedge (m + n) = (-1) \wedge r$
 $\langle \text{proof} \rangle$

lemma *Quadratic-Reciprocity*:
 $\text{Legendre } p \ q * \text{Legendre } q \ p = (-1::\text{int}) \wedge ((p - 1) \text{ div } 2 * ((q - 1) \text{ div } 2))$
 $\langle \text{proof} \rangle$

end

theorem *Quadratic-Reciprocity*:
assumes $\text{prime } p \ 2 < p \ \text{prime } q \ 2 < q \ p \neq q$
shows $\text{Legendre } p \ q * \text{Legendre } q \ p = (-1::\text{int}) \wedge ((p - 1) \text{ div } 2 * ((q - 1) \text{ div } 2))$
 $\langle \text{proof} \rangle$

theorem *Quadratic-Reciprocity-int*:
assumes $\text{prime } (\text{nat } p) \ 2 < p \ \text{prime } (\text{nat } q) \ 2 < q \ p \neq q$
shows $\text{Legendre } p \ q * \text{Legendre } q \ p = (-1::\text{int}) \wedge (\text{nat } ((p - 1) \text{ div } 2 * ((q - 1) \text{ div } 2)))$
 $\langle \text{proof} \rangle$

end

9 Pocklington's Theorem for Primes

theory *Pocklington*
imports *Residues*
begin

9.1 Lemmas about previously defined terms

lemma *prime-nat-iff''*: $\text{prime } (p::\text{nat}) \longleftrightarrow p \neq 0 \wedge p \neq 1 \wedge (\forall m. \ 0 < m \wedge m < p \longrightarrow \text{coprime } p \ m)$
 $\langle \text{proof} \rangle$

lemma *finite-number-segment*: $\text{card } \{ m. \ 0 < m \wedge m < n \} = n - 1$
 $\langle \text{proof} \rangle$

9.2 Some basic theorems about solving congruences

lemma *cong-solve*:

fixes $n :: \text{nat}$
assumes $an: \text{coprime } a \ n$
shows $\exists x. [a * x = b] \ (\text{mod } n)$
 $\langle \text{proof} \rangle$

lemma *cong-solve-unique*:

fixes $n :: \text{nat}$
assumes $an: \text{coprime } a \ n$ **and** $nz: n \neq 0$
shows $\exists! x. x < n \wedge [a * x = b] \ (\text{mod } n)$
 $\langle \text{proof} \rangle$

lemma *cong-solve-unique-nontrivial*:

fixes $p :: \text{nat}$
assumes $p: \text{prime } p$
and $pa: \text{coprime } p \ a$
and $x0: 0 < x$
and $xp: x < p$
shows $\exists! y. 0 < y \wedge y < p \wedge [x * y = a] \ (\text{mod } p)$
 $\langle \text{proof} \rangle$

lemma *cong-unique-inverse-prime*:

fixes $p :: \text{nat}$
assumes $\text{prime } p$ **and** $0 < x$ **and** $x < p$
shows $\exists! y. 0 < y \wedge y < p \wedge [x * y = 1] \ (\text{mod } p)$
 $\langle \text{proof} \rangle$

lemma *chinese-remainder-coprime-unique*:

fixes $a :: \text{nat}$
assumes $ab: \text{coprime } a \ b$ **and** $az: a \neq 0$ **and** $bz: b \neq 0$
and $ma: \text{coprime } m \ a$ **and** $nb: \text{coprime } n \ b$
shows $\exists! x. \text{coprime } x \ (a * b) \wedge x < a * b \wedge [x = m] \ (\text{mod } a) \wedge [x = n] \ (\text{mod } b)$
 $\langle \text{proof} \rangle$

9.3 Lucas's theorem

lemma *lucas-coprime-lemma*:

fixes $n :: \text{nat}$
assumes $m: m \neq 0$ **and** $am: [a^m = 1] \ (\text{mod } n)$
shows $\text{coprime } a \ n$
 $\langle \text{proof} \rangle$

lemma *lucas-weak*:

fixes $n :: \text{nat}$
assumes $n: n \geq 2$
and $an: [a^{n-1} = 1] \ (\text{mod } n)$
and $nm: \forall m. 0 < m \wedge m < n - 1 \longrightarrow \neg [a^m = 1] \ (\text{mod } n)$
shows $\text{prime } n$

$\langle proof \rangle$

lemma *nat-exists-least-iff*: $(\exists (n::nat). P\ n) \longleftrightarrow (\exists n. P\ n \wedge (\forall m < n. \neg P\ m))$
 $\langle proof \rangle$

lemma *nat-exists-least-iff'*: $(\exists (n::nat). P\ n) \longleftrightarrow P\ (Least\ P) \wedge (\forall m < (Least\ P). \neg P\ m)$
 (is ?lhs $\longleftrightarrow$?rhs)
 $\langle proof \rangle$

theorem *lucas*:

assumes *n2*: $n \geq 2$ and *an1*: $[a \frown (n - 1) = 1] \pmod n$
 and *pn*: $\forall p. \text{prime } p \wedge p \text{ dvd } n - 1 \longrightarrow [a \frown ((n - 1) \text{ div } p) \neq 1] \pmod n$
 shows *prime n*
 $\langle proof \rangle$

9.4 Definition of the order of a number mod n

definition *ord n a* = (if coprime $n\ a$ then *Least* $(\lambda d. d > 0 \wedge [a \frown d = 1] \pmod n)$ else 0)

This has the expected properties.

lemma *coprime-ord*:

fixes $n::nat$
 assumes *coprime n a*
 shows $ord\ n\ a > 0 \wedge [a \frown (ord\ n\ a) = 1] \pmod n \wedge (\forall m. 0 < m \wedge m < ord\ n\ a \longrightarrow [a \frown m \neq 1] \pmod n)$
 $\langle proof \rangle$

With the special value 0 for non-coprime case, it's more convenient.

lemma *ord-works*: $[a \frown (ord\ n\ a) = 1] \pmod n \wedge (\forall m. 0 < m \wedge m < ord\ n\ a \longrightarrow \neg [a \frown m = 1] \pmod n)$
 for $n :: nat$
 $\langle proof \rangle$

lemma *ord*: $[a \frown (ord\ n\ a) = 1] \pmod n$
 for $n :: nat$
 $\langle proof \rangle$

lemma *ord-minimal*: $0 < m \implies m < ord\ n\ a \implies \neg [a \frown m = 1] \pmod n$
 for $n :: nat$
 $\langle proof \rangle$

lemma *ord-eq-0*: $ord\ n\ a = 0 \longleftrightarrow \neg \text{coprime } n\ a$
 for $n :: nat$
 $\langle proof \rangle$

lemma *divides-rexp*: $x \text{ dvd } y \implies x \text{ dvd } (y \frown Suc\ n)$
 for $x\ y :: nat$

$\langle proof \rangle$

lemma *ord-divides*: $[a \wedge d = 1] \pmod n \longleftrightarrow \text{ord } n \ a \ \text{dvd } d$
 (is ?lhs $\longleftrightarrow$?rhs)
 for $n :: \text{nat}$
 $\langle proof \rangle$

lemma *order-divides-totient*:
 $\text{ord } n \ a \ \text{dvd } \text{totient } n$ if $\text{coprime } n \ a$
 $\langle proof \rangle$

lemma *order-divides-expdiff*:
 fixes $n :: \text{nat}$ and $a :: \text{nat}$ assumes $na: \text{coprime } n \ a$
 shows $[a \wedge d = a \wedge e] \pmod n \longleftrightarrow [d = e] \pmod{(\text{ord } n \ a)}$
 $\langle proof \rangle$

lemma *ord-not-coprime* [simp]: $\neg \text{coprime } n \ a \implies \text{ord } n \ a = 0$
 $\langle proof \rangle$

lemma *ord-1* [simp]: $\text{ord } 1 \ n = 1$
 $\langle proof \rangle$

lemma *ord-1-right* [simp]: $\text{ord } (n :: \text{nat}) \ 1 = 1$
 $\langle proof \rangle$

lemma *ord-Suc-0-right* [simp]: $\text{ord } (n :: \text{nat}) \ (\text{Suc } 0) = 1$
 $\langle proof \rangle$

lemma *ord-0-nat* [simp]: $\text{ord } 0 \ (n :: \text{nat}) = (\text{if } n = 1 \text{ then } 1 \text{ else } 0)$
 $\langle proof \rangle$

lemma *ord-0-right-nat* [simp]: $\text{ord } (n :: \text{nat}) \ 0 = (\text{if } n = 1 \text{ then } 1 \text{ else } 0)$
 $\langle proof \rangle$

lemma *ord-divides'*: $[a \wedge d = \text{Suc } 0] \pmod n = (\text{ord } n \ a \ \text{dvd } d)$
 $\langle proof \rangle$

lemma *ord-Suc-0* [simp]: $\text{ord } (\text{Suc } 0) \ n = 1$
 $\langle proof \rangle$

lemma *ord-mod* [simp]: $\text{ord } n \ (k \bmod n) = \text{ord } n \ k$
 $\langle proof \rangle$

lemma *ord-gt-0-iff* [simp]: $\text{ord } (n :: \text{nat}) \ x > 0 \longleftrightarrow \text{coprime } n \ x$
 $\langle proof \rangle$

lemma *ord-eq-Suc-0-iff*: $\text{ord } n \ (x :: \text{nat}) = \text{Suc } 0 \longleftrightarrow [x = 1] \pmod n$
 $\langle proof \rangle$

lemma *ord-cong*:

assumes $[k1 = k2] \text{ (mod } n)$

shows $\text{ord } n \ k1 = \text{ord } n \ k2$

<proof>

lemma *ord-nat-code* [*code-unfold*]:

$\text{ord } n \ a =$

$(\text{if } n = 0 \text{ then if } a = 1 \text{ then } 1 \text{ else } 0 \text{ else}$

$\text{if coprime } n \ a \text{ then } \text{Min } (\text{Set.filter } (\lambda k. [a \wedge k = 1] \text{ (mod } n)) \{0 < .. n\}) \text{ else}$

$0)$

<proof>

theorem *ord-modulus-mult-coprime*:

fixes $x :: \text{nat}$

assumes *coprime* $m \ n$

shows $\text{ord } (m * n) \ x = \text{lcm } (\text{ord } m \ x) \ (\text{ord } n \ x)$

<proof>

corollary *ord-modulus-prod-coprime*:

assumes *finite* $A \wedge i \ j. i \in A \implies j \in A \implies i \neq j \implies \text{coprime } (f \ i) \ (f \ j)$

shows $\text{ord } (\prod i \in A. f \ i :: \text{nat}) \ x = (\text{LCM } i \in A. \text{ord } (f \ i) \ x)$

<proof>

lemma *ord-power-aux*:

fixes $m \ x \ k \ a :: \text{nat}$

defines $l \equiv \text{ord } m \ a$

shows $\text{ord } m \ (a \wedge k) * \text{gcd } k \ l = l$

<proof>

theorem *ord-power*: $\text{coprime } m \ a \implies \text{ord } m \ (a \wedge k :: \text{nat}) = \text{ord } m \ a \text{ div } \text{gcd } k$
 $(\text{ord } m \ a)$

<proof>

lemma *inj-power-mod*:

assumes *coprime* $n \ (a :: \text{nat})$

shows *inj-on* $(\lambda k. a \wedge k \text{ mod } n) \{.. < \text{ord } n \ a\}$

<proof>

lemma *ord-eq-2-iff*: $\text{ord } n \ (x :: \text{nat}) = 2 \iff [x \neq 1] \text{ (mod } n) \wedge [x^2 = 1] \text{ (mod } n)$

<proof>

lemma *square-mod-8-eq-1-iff*: $[x^2 = 1] \text{ (mod } 8) \iff \text{odd } (x :: \text{nat})$

<proof>

lemma *ord-twopow-aux*:

assumes $k \geq 3$ **and** *odd* $(x :: \text{nat})$

shows $[x \wedge (2 \wedge (k - 2)) = 1] \text{ (mod } (2 \wedge k))$

<proof>

lemma *ord-twopow-3-5*:

assumes $k \geq 3 \wedge x \bmod 8 \in \{3, 5 :: \text{nat}\}$
shows $\text{ord } (2 \wedge^k) x = 2 \wedge^{k-2}$
 $\langle \text{proof} \rangle$

lemma *ord-4-3 [simp]*: $\text{ord } 4 \ (3 :: \text{nat}) = 2$
 $\langle \text{proof} \rangle$

lemma *elements-with-ord-1*: $n > 0 \implies \{x \in \text{totatives } n. \text{ord } n \ x = \text{Suc } 0\} = \{1\}$
 $\langle \text{proof} \rangle$

lemma *residue-prime-has-primroot*:

fixes $p :: \text{nat}$
assumes *prime* p
shows $\exists a \in \text{totatives } p. \text{ord } p \ a = p - 1$
 $\langle \text{proof} \rangle$

9.5 Another trivial primality characterization

lemma *prime-prime-factor*: $\text{prime } n \longleftrightarrow n \neq 1 \wedge (\forall p. \text{prime } p \wedge p \text{ dvd } n \longrightarrow p = n)$
(is ?lhs $\longleftrightarrow$?rhs)
for $n :: \text{nat}$
 $\langle \text{proof} \rangle$

lemma *prime-divisor-sqrt*: $\text{prime } n \longleftrightarrow n \neq 1 \wedge (\forall d. d \text{ dvd } n \wedge d^2 \leq n \longrightarrow d = 1)$
for $n :: \text{nat}$
 $\langle \text{proof} \rangle$

lemma *prime-prime-factor-sqrt*:
 $\text{prime } (n :: \text{nat}) \longleftrightarrow n \neq 0 \wedge n \neq 1 \wedge (\nexists p. \text{prime } p \wedge p \text{ dvd } n \wedge p^2 \leq n)$
(is ?lhs $\longleftrightarrow$?rhs)
 $\langle \text{proof} \rangle$

9.6 Pocklington theorem

lemma *pocklington-lemma*:

fixes $p :: \text{nat}$
assumes $n: n \geq 2$ **and** $nqr: n - 1 = q * r$
and $an: [a \wedge^{n-1} = 1] \ (\text{mod } n)$
and $aq: \forall p. \text{prime } p \wedge p \text{ dvd } q \longrightarrow \text{coprime } (a \wedge^{(n-1) \text{ div } p} - 1) \ n$
and $pp: \text{prime } p$ **and** $pn: p \text{ dvd } n$
shows $[p = 1] \ (\text{mod } q)$
 $\langle \text{proof} \rangle$

theorem *pocklington*:

assumes $n: n \geq 2$ **and** $nqr: n - 1 = q * r$ **and** $sqr: n \leq q^2$
and $an: [a \wedge^{n-1} = 1] \ (\text{mod } n)$

and $aq: \forall p. \text{prime } p \wedge p \text{ dvd } q \longrightarrow \text{coprime } (a^{\wedge}((n-1) \text{ div } p) - 1) \ n$
shows $\text{prime } n$
 $\langle \text{proof} \rangle$

Variant for application, to separate the exponentiation.

lemma *pocklington-alt*:

assumes $n: n \geq 2$ **and** $nqr: n - 1 = q * r$ **and** $sqr: n \leq q^2$
and $an: [a^{\wedge}(n-1) = 1] \text{ (mod } n)$
and $aq: \forall p. \text{prime } p \wedge p \text{ dvd } q \longrightarrow (\exists b. [a^{\wedge}((n-1) \text{ div } p) = b] \text{ (mod } n) \wedge$
 $\text{coprime } (b-1) \ n)$
shows $\text{prime } n$
 $\langle \text{proof} \rangle$

9.7 Prime factorizations

definition *primefact* $ps \ n \longleftrightarrow \text{foldr } (*) \ ps \ 1 = n \wedge (\forall p \in \text{set } ps. \text{prime } p)$

lemma *primefact*:

fixes $n :: \text{nat}$
assumes $n: n \neq 0$
shows $\exists ps. \text{primefact } ps \ n$
 $\langle \text{proof} \rangle$

lemma *primefact-contains*:

fixes $p :: \text{nat}$
assumes $pf: \text{primefact } ps \ n$
and $p: \text{prime } p$
and $pn: p \text{ dvd } n$
shows $p \in \text{set } ps$
 $\langle \text{proof} \rangle$

lemma *primefact-variant*: $\text{primefact } ps \ n \longleftrightarrow \text{foldr } (*) \ ps \ 1 = n \wedge \text{list-all prime } ps$
 $\langle \text{proof} \rangle$

Variant of Lucas theorem.

lemma *lucas-primefact*:

assumes $n: n \geq 2$ **and** $an: [a^{\wedge}(n-1) = 1] \text{ (mod } n)$
and $psn: \text{foldr } (*) \ ps \ 1 = n - 1$
and $psp: \text{list-all } (\lambda p. \text{prime } p \wedge \neg [a^{\wedge}((n-1) \text{ div } p) = 1] \text{ (mod } n)) \ ps$
shows $\text{prime } n$
 $\langle \text{proof} \rangle$

Variant of Pocklington theorem.

lemma *pocklington-primefact*:

assumes $n: n \geq 2$ **and** $qrn: q*r = n - 1$ **and** $nq2: n \leq q^2$
and $arnb: (a^{\wedge}r) \text{ mod } n = b$ **and** $psq: \text{foldr } (*) \ ps \ 1 = q$
and $bqn: (b^{\wedge}q) \text{ mod } n = 1$
and $psp: \text{list-all } (\lambda p. \text{prime } p \wedge \text{coprime } ((b^{\wedge}(q \text{ div } p)) \text{ mod } n - 1) \ n) \ ps$

shows prime n
 <proof>

end

10 Prime powers

theory Prime-Powers

imports Complex-Main HOL-Computational-Algebra.Primes HOL-Library.FuncSet
 begin

definition *aprimedivisor* :: 'a :: normalization-semidom $\Rightarrow$ 'a **where**
aprimedivisor q = (SOME p. prime p $\wedge$ p dvd q)

definition *primepow* :: 'a :: normalization-semidom $\Rightarrow$ bool **where**
primepow n $\longleftrightarrow$ ($\exists$ p k. prime p $\wedge$ k > 0 $\wedge$ n = p k)

definition *primepow-factors* :: 'a :: normalization-semidom $\Rightarrow$ 'a set **where**
primepow-factors n = {x. primepow x $\wedge$ x dvd n}

lemma *primepow-gt-Suc-0*: primepow n $\implies$ n > Suc 0
 <proof>

lemma

assumes prime p p dvd n
 shows prime-aprimedivisor: prime (aprimedivisor n)
 and aprimedivisor-dvd: aprimedivisor n dvd n
 <proof>

lemma

assumes n $\neq$ 0 $\neg$ is-unit (n :: 'a :: factorial-semiring)
 shows prime-aprimedivisor': prime (aprimedivisor n)
 and aprimedivisor-dvd': aprimedivisor n dvd n
 <proof>

lemma *aprimedivisor-of-prime* [simp]:

assumes prime p
 shows aprimedivisor p = p
 <proof>

lemma *aprimedivisor-pos-nat*: (n::nat) > 1 $\implies$ aprimedivisor n > 0
 <proof>

lemma *aprimedivisor-primepow-power*:

assumes primepow n k > 0
 shows aprimedivisor (n k) = aprimedivisor n
 <proof>

lemma *aprimedivisor-prime-power*:

assumes *prime* p $k > 0$
shows $\text{aprimedivisor } (p \wedge k) = p$
 <proof>

lemma *prime-factorization-primelow*:
assumes *primelow* n
shows $\text{prime-factorization } n =$
 $\text{replicate-mset } (\text{multiplicity } (\text{aprimedivisor } n) \ n) \ (\text{aprimedivisor } n)$
 <proof>

lemma *primelow-decompose*:
fixes $n :: 'a :: \text{factorial-semiring-multiplicative}$
assumes *primelow* n
shows $\text{aprimedivisor } n \wedge \text{multiplicity } (\text{aprimedivisor } n) \ n = n$
 <proof>

lemma *prime-power-not-one*:
assumes *prime* p $k > 0$
shows $p \wedge k \neq 1$
 <proof>

lemma *zero-not-primelow* [simp]: $\neg \text{primelow } 0$
 <proof>

lemma *one-not-primelow* [simp]: $\neg \text{primelow } 1$
 <proof>

lemma *primelow-not-unit* [simp]: $\text{primelow } p \implies \neg \text{is-unit } p$
 <proof>

lemma *not-primelow-Suc-0-nat* [simp]: $\neg \text{primelow } (\text{Suc } 0)$
 <proof>

lemma *primelow-gt-0-nat*: $\text{primelow } n \implies n > (0 :: \text{nat})$
 <proof>

lemma *unit-factor-primelow*:
fixes $p :: 'a :: \text{factorial-semiring-multiplicative}$
shows $\text{primelow } p \implies \text{unit-factor } p = 1$
 <proof>

lemma *aprimedivisor-primelow*:
assumes *prime* p $p \text{ dvd } n$ *primelow* $(n :: 'a :: \text{factorial-semiring-multiplicative})$
shows $\text{aprimedivisor } (p * n) = p \text{ aprimedivisor } n = p$
 <proof>

lemma *power-eq-prime-powerD*:
fixes $p :: 'a :: \text{factorial-semiring}$
assumes *prime* p $n > 0$ $x \wedge n = p \wedge k$

shows $\exists i. \text{normalize } x = \text{normalize } (p \wedge i)$
 <proof>

lemma *primepow-power-iff*:
fixes $p :: 'a :: \text{factorial-semiring-multiplicative}$
assumes $\text{unit-factor } p = 1$
shows $\text{primepow } (p \wedge n) \longleftrightarrow \text{primepow } p \wedge n > 0$
 <proof>

lemma *primepow-power-iff-nat*:
 $p > 0 \implies \text{primepow } (p \wedge n) \longleftrightarrow \text{primepow } (p :: \text{nat}) \wedge n > 0$
 <proof>

lemma *primepow-prime [simp]*: $\text{prime } n \implies \text{primepow } n$
 <proof>

lemma *primepow-prime-power [simp]*:
 $\text{prime } (p :: 'a :: \text{factorial-semiring-multiplicative}) \implies \text{primepow } (p \wedge n) \longleftrightarrow n > 0$
 <proof>

lemma *aprimedivisor-vimage*:
assumes $\text{prime } (p :: 'a :: \text{factorial-semiring-multiplicative})$
shows $\text{aprimedivisor } -' \{p\} \cap \text{primepow-factors } n = \{p \wedge k \mid k. k > 0 \wedge p \wedge k \text{ dvd } n\}$
 <proof>

lemma *aprimedivisor-nat*:
assumes $n \neq (\text{Suc } 0 :: \text{nat})$
shows $\text{prime } (\text{aprimedivisor } n) \text{ aprimedivisor } n \text{ dvd } n$
 <proof>

lemma *aprimedivisor-gt-Suc-0*:
assumes $n \neq \text{Suc } 0$
shows $\text{aprimedivisor } n > \text{Suc } 0$
 <proof>

lemma *aprimedivisor-le-nat*:
assumes $n > \text{Suc } 0$
shows $\text{aprimedivisor } n \leq n$
 <proof>

lemma *bij-betw-primewords*:
 $\text{bij-betw } (\lambda(p,k). p \wedge \text{Suc } k :: 'a :: \text{factorial-semiring-multiplicative})$
 (Collect prime $\times$ UNIV) (Collect primepow)
 <proof>

lemma *primepow-multD*:
 assumes *primepow* ($a * b :: \text{nat}$)
 shows $a = 1 \vee \text{primepow } a \wedge b = 1 \vee \text{primepow } b$
 $\langle \text{proof} \rangle$

lemma *primepow-mult-aprime divisorI*:
 assumes *primepow* ($n :: 'a :: \text{factorial-semiring-multiplicative}$)
 shows *primepow* (*aprime divisor* $n * n$)
 $\langle \text{proof} \rangle$

lemma *primepow-factors-altdef*:
 fixes $x :: 'a :: \text{factorial-semiring-multiplicative}$
 assumes $x \neq 0$
 shows *primepow-factors* $x = \{p \wedge k \mid p \in \text{prime-factors } x \wedge k \in \{0 < .. \text{multiplicity } p \ x\}\}$
 $\langle \text{proof} \rangle$

lemma *finite-primepow-factors*:
 assumes $x \neq (0 :: 'a :: \text{factorial-semiring-multiplicative})$
 shows *finite* (*primepow-factors* x)
 $\langle \text{proof} \rangle$

lemma *aprime divisor-primepow-factors-conv-prime-factorization*:
 assumes [*simp*]: $n \neq (0 :: 'a :: \text{factorial-semiring-multiplicative})$
 shows *image-mset* *aprime divisor* (*mset-set* (*primepow-factors* n)) = *prime-factorization* n
 (*is* ?*lhs* = ?*rhs*)
 $\langle \text{proof} \rangle$

lemma *prime-elem-aprime divisor-nat*: $d > \text{Suc } 0 \implies \text{prime-elem } (\text{aprime divisor } d)$
 $\langle \text{proof} \rangle$

lemma *aprime divisor-gt-0-nat* [*simp*]: $d > \text{Suc } 0 \implies \text{aprime divisor } d > 0$
 $\langle \text{proof} \rangle$

lemma *aprime divisor-gt-Suc-0-nat* [*simp*]: $d > \text{Suc } 0 \implies \text{aprime divisor } d > \text{Suc } 0$
 $\langle \text{proof} \rangle$

lemma *aprime divisor-not-Suc-0-nat* [*simp*]: $d > \text{Suc } 0 \implies \text{aprime divisor } d \neq \text{Suc } 0$
 $\langle \text{proof} \rangle$

lemma *multiplicity-aprime divisor-gt-0-nat* [*simp*]:
 $d > \text{Suc } 0 \implies \text{multiplicity } (\text{aprime divisor } d) \ d > 0$
 $\langle \text{proof} \rangle$

lemma *primepowI*:

$prime\ p \implies k > 0 \implies p \wedge^k = n \implies primepow\ n \wedge a_{prime}divisor\ n = p$
 <proof>

lemma *not-primepowI*:
 assumes $prime\ p\ prime\ q\ p \neq q\ p\ dvd\ n\ q\ dvd\ n$
 shows $\neg primepow\ n$
 <proof>

lemma *sum-prime-factorization-conv-sum-primepow-factors*:
 fixes $n :: 'a :: factorial-semiring-multiplicative$
 assumes $n \neq 0$
 shows $(\sum_{q \in primepow-factors\ n} f\ (a_{prime}divisor\ q)) = (\sum_{p \in \#prime-factorization\ n} f\ p)$
 <proof>

lemma *multiplicity-aprime divisor-Suc-0-iff*:
 assumes $primepow\ (n :: 'a :: factorial-semiring-multiplicative)$
 shows $multiplicity\ (a_{prime}divisor\ n)\ n = Suc\ 0 \longleftrightarrow prime\ n$
 <proof>

definition *mangoldt* :: $nat \Rightarrow 'a :: real-algebra-1$ **where**
 $mangoldt\ n = (if\ primepow\ n\ then\ of-real\ (ln\ (real\ (a_{prime}divisor\ n)))\ else\ 0)$

lemma *mangoldt-0 [simp]*: $mangoldt\ 0 = 0$
 <proof>

lemma *mangoldt-Suc-0 [simp]*: $mangoldt\ (Suc\ 0) = 0$
 <proof>

lemma *of-real-mangoldt [simp]*: $of-real\ (mangoldt\ n) = mangoldt\ n$
 <proof>

lemma *mangoldt-sum*:
 assumes $n \neq 0$
 shows $(\sum d \mid d\ dvd\ n. mangoldt\ d :: 'a :: real-algebra-1) = of-real\ (ln\ (real\ n))$
 <proof>

lemma *mangoldt-primepow*:
 $prime\ p \implies mangoldt\ (p \wedge^k) = (if\ k > 0\ then\ of-real\ (ln\ (real\ p))\ else\ 0)$
 <proof>

lemma *mangoldt-primepow' [simp]*: $prime\ p \implies k > 0 \implies mangoldt\ (p \wedge^k) = of-real\ (ln\ (real\ p))$
 <proof>

lemma *mangoldt-prime [simp]*: $prime\ p \implies mangoldt\ p = of-real\ (ln\ (real\ p))$
 <proof>

lemma *mangoldt-nonneg*: $0 \leq (\text{mangoldt } d :: \text{real})$
 ⟨proof⟩

lemma *norm-mangoldt* [simp]:
 $\text{norm } (\text{mangoldt } n :: 'a :: \text{real-normed-algebra-1}) = \text{mangoldt } n$
 ⟨proof⟩

lemma *Re-mangoldt* [simp]: $\text{Re } (\text{mangoldt } n) = \text{mangoldt } n$
and *Im-mangoldt* [simp]: $\text{Im } (\text{mangoldt } n) = 0$
 ⟨proof⟩

lemma *abs-mangoldt* [simp]: $\text{abs } (\text{mangoldt } n :: \text{real}) = \text{mangoldt } n$
 ⟨proof⟩

lemma *mangoldt-le*:
 assumes $n > 0$
 shows $\text{mangoldt } n \leq \ln n$
 ⟨proof⟩

end

11 Primitive roots in residue rings and Carmichael's function

theory *Residue-Primitive-Roots*
 imports *Pocklington*
 begin

This theory develops the notions of primitive roots (generators) in residue rings. It also provides a definition and all the basic properties of Carmichael's function $\lambda(n)$, which is strongly related to this. The proofs mostly follow Apostol's presentation

11.1 Primitive roots in residue rings

A primitive root of a residue ring modulo n is an element g that *generates* the ring, i. e. such that for each x coprime to n there exists an i such that $x = g^i$. A simpler definition is that g must have the same order as the cardinality of the multiplicative group, which is $\varphi(n)$.

Note that for convenience, this definition does *not* demand $g < n$.

inductive *residue-primroot* :: $\text{nat} \Rightarrow \text{nat} \Rightarrow \text{bool}$ **where**
 $n > 0 \implies \text{coprime } n \ g \implies \text{ord } n \ g = \text{totient } n \implies \text{residue-primroot } n \ g$

lemma *residue-primroot-def* [code]:
 $\text{residue-primroot } n \ x \longleftrightarrow n > 0 \wedge \text{coprime } n \ x \wedge \text{ord } n \ x = \text{totient } n$
 ⟨proof⟩

lemma *not-residue-primroot-0* [simp]: $\sim \text{residue-primroot } 0 \ x$
 <proof>

lemma *residue-primroot-mod* [simp]: $\text{residue-primroot } n \ (x \bmod n) = \text{residue-primroot } n \ x$
 <proof>

lemma *residue-primroot-cong*:
 assumes $[x = x'] \ (mod \ n)$
 shows $\text{residue-primroot } n \ x = \text{residue-primroot } n \ x'$
 <proof>

lemma *not-residue-primroot-0-right* [simp]: $\text{residue-primroot } n \ 0 \longleftrightarrow n = 1$
 <proof>

lemma *residue-primroot-1-iff*: $\text{residue-primroot } n \ (\text{Suc } 0) \longleftrightarrow n \in \{1, 2\}$
 <proof>

11.2 Primitive roots modulo a prime

For prime p , we now analyse the number of elements in the ring $\mathbb{Z}/p\mathbb{Z}$ whose order is precisely d for each d .

context
 fixes $n :: nat$ and ψ
 assumes $n: n > 1$
 defines $\psi \equiv (\lambda d. \text{card } \{x \in \text{totatives } n. \text{ord } n \ x = d\})$
begin

lemma *elements-with-ord-restrict-totatives*:
 $d > 0 \implies \{x \in \{..<n\}. \text{ord } n \ x = d\} = \{x \in \text{totatives } n. \text{ord } n \ x = d\}$
 <proof>

lemma *prime-elements-with-ord*:
 assumes $\psi \ d \neq 0$ and *prime* n
 and $a: a \in \text{totatives } n \ \text{ord } n \ a = d \ a \neq 1$
 shows $\text{inj-on } (\lambda k. a \wedge^k \bmod n) \ \{..<d\}$
 and $\{x \in \{..<n\}. [x \wedge^d = 1] \ (mod \ n)\} = (\lambda k. a \wedge^k \bmod n) \ ` \ \{..<d\}$
 and $\text{bij-betw } (\lambda k. a \wedge^k \bmod n) \ (\text{totatives } d) \ \{x \in \{..<n\}. \text{ord } n \ x = d\}$
 <proof>

lemma *prime-card-elements-with-ord*:
 assumes $\psi \ d \neq 0$ and *prime* n
 shows $\psi \ d = \text{totient } d$
 <proof>

lemma *prime-sum-card-elements-with-ord-eq-totient*:
 $(\sum d \mid d \text{ dvd } \text{totient } n. \psi \ d) = \text{totient } n$
 <proof>

We can now show that the number of elements of order d is $\varphi(d)$ if $d \mid p-1$ and 0 otherwise.

theorem *prime-card-elements-with-ord-eq-totient:*

assumes *prime* n

shows $\psi\ d = (\text{if } d \text{ dvd } n - 1 \text{ then totient } d \text{ else } 0)$

<proof>

As a corollary, we get that the number of primitive roots modulo a prime p is $\varphi(p-1)$. Since this number is positive, we also get that there *is* at least one primitive root modulo p .

lemma

assumes *prime* n

shows *prime-card-primitive-roots:* $\text{card } \{x \in \text{totatives } n. \text{ord } n\ x = n - 1\} = \text{totient } (n - 1)$

$\text{card } \{x \in \{..<n\}. \text{ord } n\ x = n - 1\} = \text{totient } (n - 1)$

and *prime-primitive-root-exists:* $\exists x. \text{residue-primroot } n\ x$

<proof>

end

11.3 Primitive roots modulo powers of an odd prime

Any primitive root g modulo an odd prime p is also a primitive root modulo p^k for all $k > 0$ if $[g^{p-1} \neq 1] \pmod{p^2}$. To show this, we first need the following lemma.

lemma *residue-primroot-power-prime-power-neq-1:*

assumes $k \geq 2$

assumes p : *prime* p *odd* p **and** *residue-primroot* $p\ g$ **and** $[g \wedge (p-1) \neq 1] \pmod{p^2}$

shows $[g \wedge \text{totient } (p \wedge (k-1)) \neq 1] \pmod{(p \wedge k)}$

<proof>

We can now show that primitive roots modulo p with the above condition are indeed also primitive roots modulo p^k .

proposition *residue-primroot-prime-lift-iff:*

assumes p : *prime* p *odd* p **and** *residue-primroot* $p\ g$

shows $(\forall k > 0. \text{residue-primroot } (p \wedge k)\ g) \longleftrightarrow [g \wedge (p-1) \neq 1] \pmod{p^2}$

<proof>

If p is an odd prime, there is always a primitive root g modulo p , and if g does not fulfil the above assumption required for it to be liftable to p^k , we can use $g + p$, which is also a primitive root modulo p and *does* fulfil the assumption.

This shows that any modulus that is a power of an odd prime has a primitive root.

theorem *residue-primroot-odd-prime-power-exists:*

assumes p : prime p odd p
obtains g **where** $\forall k > 0. \text{residue-primroot } (p \wedge k) g$
 $\langle \text{proof} \rangle$

11.4 Carmichael's function

Carmichael's function $\lambda(n)$ gives the LCM of the orders of all elements in the residue ring modulo n – or, equivalently, the maximum order, as we will show later. Algebraically speaking, it is the exponent of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$.

It is not to be confused with Liouville's function, which is also denoted by $\lambda(n)$.

definition *Carmichael* **where**

Carmichael $n = (\text{LCM } a \in \text{totatives } n. \text{ord } n a)$

lemma *Carmichael-0* [simp]: *Carmichael* 0 = 1
 $\langle \text{proof} \rangle$

lemma *Carmichael-1* [simp]: *Carmichael* 1 = 1
 $\langle \text{proof} \rangle$

lemma *Carmichael-Suc-0* [simp]: *Carmichael* (Suc 0) = 1
 $\langle \text{proof} \rangle$

lemma *ord-dvd-Carmichael*:

assumes $n > 1$ coprime $n k$

shows $\text{ord } n k \text{ dvd } \text{Carmichael } n$

$\langle \text{proof} \rangle$

lemma *Carmichael-divides*:

assumes *Carmichael* $n \text{ dvd } k$ coprime $n a$

shows $[a \wedge k = 1] \pmod n$

$\langle \text{proof} \rangle$

lemma *Carmichael-dvd-totient*: *Carmichael* $n \text{ dvd } \text{totient } n$
 $\langle \text{proof} \rangle$

lemma *Carmichael-dvd-mono-coprime*:

assumes coprime $m n$ $m > 1$ $n > 1$

shows *Carmichael* $m \text{ dvd } \text{Carmichael } (m * n)$

$\langle \text{proof} \rangle$

λ distributes over the product of coprime numbers similarly to φ , but with LCM instead of multiplication:

lemma *Carmichael-mult-coprime*:

assumes coprime $m n$

shows *Carmichael* $(m * n) = \text{lcm } (\text{Carmichael } m) (\text{Carmichael } n)$

$\langle \text{proof} \rangle$

lemma *Carmichael-pos* [*simp*, *intro*]: $\text{Carmichael } n > 0$
 $\langle \text{proof} \rangle$

lemma *Carmichael-nonzero* [*simp*]: $\text{Carmichael } n \neq 0$
 $\langle \text{proof} \rangle$

lemma *power-Carmichael-eq-1*:
assumes $n > 1$ *coprime* n x
shows $[x \wedge \text{Carmichael } n = 1] \pmod n$
 $\langle \text{proof} \rangle$

lemma *Carmichael-2* [*simp*]: $\text{Carmichael } 2 = 1$
 $\langle \text{proof} \rangle$

lemma *Carmichael-4* [*simp*]: $\text{Carmichael } 4 = 2$
 $\langle \text{proof} \rangle$

lemma *residue-primroot-Carmichael*:
assumes *residue-primroot* n g
shows $\text{Carmichael } n = \text{totient } n$
 $\langle \text{proof} \rangle$

lemma *Carmichael-odd-prime-power*:
assumes *prime* p *odd* p $k > 0$
shows $\text{Carmichael } (p \wedge k) = p \wedge (k - 1) * (p - 1)$
 $\langle \text{proof} \rangle$

lemma *Carmichael-prime*:
assumes *prime* p
shows $\text{Carmichael } p = p - 1$
 $\langle \text{proof} \rangle$

lemma *Carmichael-twopow-ge-8*:
assumes $k \geq 3$
shows $\text{Carmichael } (2 \wedge k) = 2 \wedge (k - 2)$
 $\langle \text{proof} \rangle$

lemma *Carmichael-twopow*:
 $\text{Carmichael } (2 \wedge k) = (\text{if } k \leq 2 \text{ then } 2 \wedge (k - 1) \text{ else } 2 \wedge (k - 2))$
 $\langle \text{proof} \rangle$

lemma *Carmichael-prime-power*:
assumes *prime* p $k > 0$
shows $\text{Carmichael } (p \wedge k) =$
 $(\text{if } p = 2 \wedge k > 2 \text{ then } 2 \wedge (k - 2) \text{ else } p \wedge (k - 1) * (p - 1))$
 $\langle \text{proof} \rangle$

lemma *Carmichael-prod-coprime*:

assumes *finite* $A \wedge i, j. i \in A \implies j \in A \implies i \neq j \implies \text{coprime } (f\ i) (f\ j)$
shows $\text{Carmichael } (\prod_{i \in A} f\ i) = (\text{LCM } i \in A. \text{Carmichael } (f\ i))$
 $\langle \text{proof} \rangle$

Since λ distributes over coprime factors and we know the value of $\lambda(p^k)$ for prime p , we can now give a closed formula for $\lambda(n)$ in terms of the prime factorisation of n :

theorem *Carmichael-closed-formula:*

$\text{Carmichael } n =$
 $(\text{LCM } p \in \text{prime-factors } n. \text{let } k = \text{multiplicity } p\ n$
 $\text{in if } p = 2 \wedge k > 2 \text{ then } 2^{k-2} \text{ else } p^{k-1} * (p-1))$
 $(\text{is } - = \text{Lcm } ?A)$
 $\langle \text{proof} \rangle$

corollary *even-Carmichael:*

assumes $n > 2$
shows $\text{even } (\text{Carmichael } n)$
 $\langle \text{proof} \rangle$

lemma *eval-Carmichael:*

assumes *prime-factorization* $n = A$
shows $\text{Carmichael } n = (\text{LCM } p \in \text{set-mset } A.$
 $\text{let } k = \text{count } A\ p \text{ in if } p = 2 \wedge k > 2 \text{ then } 2^{k-2} \text{ else } p^{k-1} * (p-1))$
 $\langle \text{proof} \rangle$

Any residue ring always contains a λ -root, i.e. an element whose order is $\lambda(n)$.

theorem *Carmichael-root-exists:*

assumes $n > (0::\text{nat})$
obtains g **where** $g \in \text{totatives } n$ **and** $\text{ord } n\ g = \text{Carmichael } n$
 $\langle \text{proof} \rangle$

This also means that the Carmichael number is not only the LCM of the orders of the elements of the residue ring, but indeed the maximum of the orders.

lemma *Carmichael-altdef:*

$\text{Carmichael } n = (\text{if } n = 0 \text{ then } 1 \text{ else } \text{Max } (\text{ord } n \text{ ' totatives } n))$
 $\langle \text{proof} \rangle$

11.5 Existence of primitive roots for general moduli

We now related Carmichael's function to the existence of primitive roots and, in the end, use this to show precisely which moduli have primitive roots and which do not.

The first criterion for the existence of a primitive root is this: A primitive root modulo n exists iff $\lambda(n) = \varphi(n)$.

lemma *Carmichael-eq-totient-imp-primroot:*
assumes $n > 0$ **and** $\text{Carmichael } n = \text{totient } n$
shows $\exists g. \text{residue-primroot } n \ g$
 $\langle \text{proof} \rangle$

theorem *residue-primroot-iff-Carmichael:*
 $(\exists g. \text{residue-primroot } n \ g) \longleftrightarrow \text{Carmichael } n = \text{totient } n \wedge n > 0$
 $\langle \text{proof} \rangle$

Any primitive root modulo mn for coprime m, n is also a primitive root modulo m and n . The converse does not hold in general.

lemma *residue-primroot-modulus-mult-coprimeD:*
assumes $\text{coprime } m \ n$ **and** $\text{residue-primroot } (m * n) \ g$
shows $\text{residue-primroot } m \ g \ \text{residue-primroot } n \ g$
 $\langle \text{proof} \rangle$

If a primitive root modulo mn exists for coprime m, n , then $\lambda(m)$ and $\lambda(n)$ must also be coprime. This is helpful in establishing that there are no primitive roots modulo mn by showing e.g. that $\lambda(m)$ and $\lambda(n)$ are both even.

lemma *residue-primroot-modulus-mult-coprime-imp-Carmichael-coprime:*
assumes $\text{coprime } m \ n$ **and** $\text{residue-primroot } (m * n) \ g$
shows $\text{coprime } (\text{Carmichael } m) \ (\text{Carmichael } n)$
 $\langle \text{proof} \rangle$

The following moduli are precisely those that have primitive roots.

definition *cyclic-moduli :: nat set where*
 $\text{cyclic-moduli} = \{1, 2, 4\} \cup \{p^k \mid p \text{ prime } p \wedge \text{odd } p \wedge k > 0\} \cup$
 $\{2 * p^k \mid p \text{ prime } p \wedge \text{odd } p \wedge k > 0\}$

theorem *residue-primroot-iff-in-cyclic-moduli:*
 $(\exists g. \text{residue-primroot } m \ g) \longleftrightarrow m \in \text{cyclic-moduli}$
 $\langle \text{proof} \rangle$

lemma *residue-primroot-is-generator:*
assumes $m > 1$ **and** $\text{residue-primroot } m \ g$
shows $\text{bij-betw } (\lambda i. g^i \text{ mod } m) \ \{..<\text{totient } m\} \ (\text{totatives } m)$
 $\langle \text{proof} \rangle$

Given one primitive root g , all the primitive roots are powers g^i for $1 \leq i \leq \varphi(n)$ with $\gcd(i, \varphi(n)) = 1$.

theorem *residue-primroot-bij-betw-primroots:*
assumes $m > 1$ **and** $\text{residue-primroot } m \ g$
shows $\text{bij-betw } (\lambda i. g^i \text{ mod } m) \ (\text{totatives } (\text{totient } m))$
 $\{g \in \text{totatives } m. \text{residue-primroot } m \ g\}$
 $\langle \text{proof} \rangle$

It follows from the above statement that any residue ring modulo n that has primitive roots has exactly $\varphi(\varphi(n))$ of them.

corollary *card-residue-primroots:*
assumes $\exists g. \text{residue-primroot } m \ g$
shows $\text{card } \{g \in \text{totatives } m. \text{residue-primroot } m \ g\} = \text{totient } (\text{totient } m)$
 $\langle \text{proof} \rangle$

corollary *card-residue-primroots':*
 $\text{card } \{g \in \text{totatives } m. \text{residue-primroot } m \ g\} =$
 $(\text{if } m \in \text{cyclic-moduli} \text{ then } \text{totient } (\text{totient } m) \text{ else } 0)$
 $\langle \text{proof} \rangle$

As an example, we evaluate $\lambda(122200)$ using the prime factorisation.

lemma *Carmichael* $122200 = 1380$
 $\langle \text{proof} \rangle$

end

12 Comprehensive number theory

theory *Number-Theory*
imports
Fib
Residues
Eratosthenes
Mod-Exp
Quadratic-Reciprocity
Pocklington
Prime-Powers
Residue-Primitive-Roots
begin

end