P8: product of odd integers

Goal: $\forall m, n \in \mathbb{Z} : (m, n \text{ odd} \Longrightarrow m \cdot n \text{ odd})$

Assume:
1. $m, n \in \mathbb{Z}$
2. m, n odd

$$\begin{aligned} m &= 2a + 1 \\ n &= 2b + 1 \\ m \cdot n &= 2(2ab + a + b) + 1 \end{aligned}$$

P10: rational square root

Goal: $\forall x \in \mathbb{R}^+ : \sqrt{x} \text{ rational} \Longrightarrow x \text{ rational}$

Assume:
1. $x \in \mathbb{R}^+$
2. $\sqrt{x}$ rational

$$\begin{aligned} \sqrt{x} &= \frac{p}{q} \\ x &= \frac{p^2}{q^2} \end{aligned}$$

T11: transitivity of implication

Goal: $\forall P_1, P_2, P_3 : ((P_1 \Longrightarrow P_2) \land (P_2 \Longrightarrow P_3) \Longrightarrow (P_1 \Longrightarrow P_3))$

Assume:
1. $P_1 \Longrightarrow P_2$
2. $P_2 \Longrightarrow P_3$
3. P_1

$$\begin{aligned} &\Longrightarrow P_2 \text{ by } (1) \\ &\Longrightarrow P_3 \text{ by } (2) \end{aligned}$$

P18: linearaity of congruence

Goal: $\forall m, n \in \mathbb{Z}^+ \land a, b \in \mathbb{Z} : a \equiv b \pmod{m} \Longleftrightarrow n \cdot a \equiv n \cdot b \pmod{n \cdot m}$

Assume:
1. $m, n \in \mathbb{Z}^+$
2. $a, b \in \mathbb{Z}$

$$\begin{aligned} a \equiv b \pmod{m} &\Longleftrightarrow a - b = k \cdot m \\ &\Longleftrightarrow n \cdot a - n \cdot b = k \cdot n \cdot m \\ &\Longleftrightarrow n \cdot a \equiv n \cdot b \pmod{n \cdot m} \end{aligned}$$

T19: 6 divisible

Goal: $\forall n \in \mathbb{Z} : (6|n \Longleftrightarrow 2|n \land 3|n)$

Assume:
1. $n \in \mathbb{Z}$

$$\begin{aligned} 6|n &\implies n = 6k \\ &\implies n = 3 \cdot (2k) \land n = 2 \cdot (3k) \\ &\implies 3|n \land 2|n \end{aligned}$$

$$\begin{aligned} n &= 2a \\ n &= 3b \\ 3n &= 6a \\ 2n &= 6b \\ n &= 6(a-b) \\ &\implies 6|n \end{aligned}$$

P21

Goal: $\forall k \in \mathbb{Z}^+ : \left(\exists i, j \in \mathbb{Z} : 4k = i^2 - j^2\right)$

Assume:

1. $k \in \mathbb{Z}+$

Let $i = k + 1$ and $j = k - 1$, then $i^2 - j^2 = 4k$

T23: transitivity of divisiblity

Goal: $\forall l, m, n \in \mathbb{Z} : (l|m \land m|n \implies l|n)$

Assume:

1. $l, m, k \in \mathbb{Z}$
2. $l|m \land m|n$

$$\begin{aligned} m &= a \cdot l \\ n &= b \cdot m \\ n &= (a \cdot b) \cdot l \\ &\implies 1|n \end{aligned}$$

T24: uniqueness of congruence

Goal: $\forall m \in \mathbb{Z}^+ \land n \in \mathbb{Z} : (\exists! z : 0 \leq z < m \land z \equiv n \pmod{m})$

Assume:

1. $m \in \mathbb{Z}^+ \land n \in \mathbb{Z}$

Missing

Goal: $\exists z : 0 \leq z < m \land z \equiv n \pmod{m}$

Assume:

1. $0 \leq z < m \land z \equiv n \pmod{m}$
2. $0 \leq z' < m \land z' \equiv n \pmod{m}$

$$\begin{aligned} & z \equiv z' \pmod{m} \\ \implies & z - z' = k \cdot m \\ & -m < z - z' < m \\ \implies & k = 0 \\ \implies & z = z' \end{aligned}$$

P25: square modulo 4

Goal: $\forall n \in \mathbb{Z} : n^2 \equiv 0 \pmod{4} \lor n^2 \equiv 1 \pmod{4}$

Case $n = 2k$

$n^2 \equiv 4k^2 \equiv 0 \pmod{4}$

Case $n = 2k + 1$

$n^2 \equiv 4k^2 + 4k + 1 \equiv 1 \pmod{4}$

L27: ends of combinations

Goal: $\forall p \in \mathbb{Z}^+ \land m \in \mathbb{N} : \left(m = 0 \lor m = p \Longrightarrow \binom{p}{m} \equiv 1 \pmod{p}\right)$

Assume:
1. $p \in \mathbb{Z}^+ \land m \in \mathbb{N}$

Case: $m = 0$

$$\binom{p}{0} \equiv 1 \pmod{p}$$

Case: $m = p$

$$\binom{p}{0} \equiv 1 \pmod{p}$$

L28: non-ends of combinations

Goal: $\forall p \text{ prime} \land m \in \mathbb{Z} : \left(0 < m < p \Longrightarrow \binom{p}{m} \equiv 0 \pmod{p}\right)$

Assume:
1. p prime $\land\, m \in \mathbb{Z}$
2. $0 < m < p$

$$\begin{aligned} \binom{p}{m} &\equiv \frac{p!}{(p-m)!m!} \\ &\equiv p \cdot \frac{(p-1)!}{(p-m)!m!} \\ &\equiv 0 \pmod{p} \end{aligned}$$

As p is only cancelled if a prime factor of p is in $(p-m)!m!$, the only prime factors of p are 1 and p, all prime factors of $(p-m)!m!$ are less than p.

P29: ends and non-ends of combinations

Goal: $\forall p \text{ prime} \land m \in \mathbb{Z} \land 0 \leq m \leq p : \binom{p}{m} \equiv 0 \pmod{p} \lor \binom{p}{m} \equiv 1 \pmod{p}$

Assume:
1. p prime $\land\, m \in \mathbb{Z}$
2. $0 \leq m \leq p$

Case: $m = 0 \lor m = p$

$$\binom{p}{m} \equiv 1 \pmod{p}$$

Case $0 < m < p$

$$\binom{p}{m} \equiv 0 \pmod{p}$$

C33: the freshman's dream

Goal: $\forall m, n \in \mathbb{N} \land p \text{ prime} : (m+n)^p \equiv m^p + n^p \pmod{p}$

Assume:
1. $m, n \in \mathbb{N} \land p$ prime

$$\begin{aligned} (m+n)^p &\equiv \sum_{k=1}^{p} \binom{p}{k} m^{p-k} n^k \\ &\equiv m^p + n^p \pmod{p} \end{aligned}$$

C34: the dropout lemma

Goal: $\forall m \in \mathbb{N} \land p \text{ prime} : (m+1)^p \equiv m^p + 1 \pmod{p}$

Special case of (C33), $n = 1$

C35: the many dropout lemma

Goal: $\forall m, i \in \mathbb{N} \land p \text{ prime} : (m+i)^p \equiv m^p + 1 \pmod{p}$

Assume:

1. $m, i \in \mathbb{N}$
2. p prime

$$\begin{aligned}(m+i)^p &\equiv (m+i-1)^p + 1 \\ &\equiv (m+i-2)^p + 1 + 1 \\ &\vdots \\ &\equiv m^p + i \pmod{p}\end{aligned}$$

T36: Fermat's little theorem (clause 1)

Goal 1: $\forall i \in \mathbb{N} \land p \text{ prime} : i^p \equiv i \pmod{p}$

Special case of (C35), $m = 0$

T36: Fermat's little theorem (clause 2)

Goal 2: $\forall i \in \mathbb{N} \land p \text{ prime} \land p \nmid i : i^{p-1} \equiv 1 \pmod{p}$

Assume:

1. $i \in n \land p \text{ prime} \land p \nmid i$

$$\begin{aligned}i^p \equiv i \pmod{p} &\Longrightarrow \exists k \in \mathbb{Z} : i^p - i = kp \\ &\Longrightarrow i^{p-1} - 1 = (k/i)p \quad \text{as } p \nmid i \\ &\Longrightarrow i^{p-1} \equiv 1 \pmod{p}\end{aligned}$$

C40: the contrapositive

Goal: $(P \Longrightarrow Q) \Longleftrightarrow (\neg Q \Longrightarrow \neg P)$

Assume:

1. $P \Longrightarrow Q$
2. $\neg Q$

Suppose P, then Q. By contradiction: $\neg P$

Assume:

1. $\neg Q \Longrightarrow \neg P$
2. P

Suppose $\neg Q$, then $\neg P$. By contradiction: Q

C41: irrational square root

Goal: $\forall x \notin \mathbb{Q} : \sqrt{x} \notin \mathbb{Q}$

Assume:

1. $x \notin \mathbb{Q}$

Suppose $\sqrt{x} \in \mathbb{Q}$, then $x \in \mathbb{Q}$. By contradiction: $\sqrt{x} \notin \mathbb{Q}$

C42: rational lowest terms

Goal: $x \in \mathbb{Q} \Longleftrightarrow \exists m, n \in \mathbb{Z}^+ : x = m/n \land \neg(\exists p \text{ prime} : p|m \land p|n)$

Assume:

1. $x \in \mathbb{Q}$

Suppose $\forall m, n \in \mathbb{Z}^+ \land x = m/n : (\exists p \text{ prime} : p|m \land p|n)$

$$\begin{aligned}
x &= \frac{m}{n} \quad \text{by } (1) \\
\implies &\exists p_1 \text{ prime} : p|m \land p|n \\
\implies &m = p_1 m' \land n = p_1 n' \\
\implies &m = p_1 p_2 m'' \land n = p_1 p_2 n'' \quad \text{by running the same argument on } x' = m'/n' \\
&\vdots
\end{aligned}$$

Then m and n are products of infinitely many primes. All positive integers are product of finitely many primes. So by contradiction: $\exists m, n \in \mathbb{Z}^+ : x = m/n \land \neg(\exists p \text{ prime} : p|m \land p|n)$

P47: equality of inverses

Goal: For a monoid $(e, \cdot)$, an element x admits an inverse if its left and right inverses are equal.

$$\begin{aligned}
r &= (l \cdot x) \cdot r \\
&= l \cdot (x \cdot r) \\
&= l
\end{aligned}$$

T53: division theorem

Goal: $\forall m \in \mathbb{N}, n \in \mathbb{Z}^+ : (\exists! q, !r \in \mathbb{Z} : q \geq 0 \land 0 \leq r < n \land m = q \cdot n + r)$

Assume:

1. $m \in \mathbb{N} \land n \in \mathbb{Z}^+$

$$\begin{aligned}
\implies &\exists! n \in \mathbb{Z} : 0 \leq r < n \land m \equiv r \pmod{n} \quad \text{by (T24: uniqueness of congruence)} \\
\implies &\exists! q \in \mathbb{Z} : m = q \cdot n + r
\end{aligned}$$

T56: correctness of `divalg`

```
let rec divalg m n =
  let diviter q r =
    if r < n then (q, r)
    else diviter (q + 1) (r - n)
  in diviter 0 n
```

Goal: `diviter` terminates

`r` decreases in the natural numbers, this cannot continue forever.

Goal: `diviter` outputs (q_0, r_0) satisfying $r_0 < n \land m = q_0 \cdot m + r_0$

All calls to `diviter` satisfies $m = q \cdot m + r$

1. `diviter 0 n`
2. `diviter 1 (n - m)`
3. `diviter 2 (n - 2 * m)`
4. $\vdots$
5. `diviter q_0 r_0`

The last call satisfies $r_0 < n$

P57: uniqueness of `rem`

```
let rem m n = let (_, r) = divalg m n in r
```

Goal: $\forall m \in \mathbb{Z}^+ \wedge k, l \in \mathbb{N} : (k \equiv l \pmod{m} \iff \text{rem}(l, m) = \text{rem}(k, m))$

Assume:

1. $m \in \mathbb{Z}^+ \wedge k, l \in \mathbb{N}$

2. $k \equiv l \pmod{m}$

$$\begin{aligned} k &= q_k \cdot m + r_k \\ l &= q_l \cdot m + r_l \end{aligned}$$

$$\begin{aligned} &\implies r_k \equiv r_l \pmod{m} \\ &\implies r_k - r_l = a \cdot m \end{aligned}$$

Again by $-m < r_k - r_l < m$ we have $a = 0$ so $r_k = r_l$.

2. $r_k = r_l$

Trivial.

C58: existence of modular integer (clause 1)

Goal: $\forall n \in \mathbb{N} : n \equiv \text{rem}(n, m) \pmod{m}$

$$\begin{aligned} & n = q \cdot m + \text{rem}(n, m) \\ \implies & n - \text{rem}(n, m) = q \cdot m \\ \implies & n \equiv \text{rem}(n, m) \pmod{m} \end{aligned}$$

C58: existence of modular integer (clause 2)

Goal: $\forall k \in \mathbb{Z} : (\exists! [k]_m : 0 \leq [k]_m < m \wedge k \equiv [k]_m \pmod{m})$

Assume:

1. $k \in \mathbb{Z}$

Existence: let $[k]_m = \text{rem}(k, m)$

Uniqueness:

$$\begin{aligned} & -m < [k]_m - {[k]_m}' < m \\ & [k]_m \equiv {[k]_m}' \pmod{m} \\ \implies & [k]_m = {[k]_m}' \end{aligned}$$

P62: the modular integers is a commutative ring

Goal: $\forall m > 1 : (\mathbb{Z}_m, 0, +_m, 1, \cdot_m)$ is a commutative ring

Assume:

1. $m > 1$

- $(\mathbb{Z}_m, 0, +_m)$ is a commutative group (trivial)
- $(\mathbb{Z}_m, 0, \cdot_m)$ is a commutative monoid (trivial)
- $\cdot_m$ distributes over $+_m$ (trivial)

P63: existence of reciprocal

Goal: $\forall k \in \mathbb{Z}_m : (k \text{ has reciprocal} \iff \exists i, j \in \mathbb{Z} : k \cdot i + m \cdot j = 1)$

Assume:

1. $k \in \mathbb{Z}_m$

$$\begin{aligned}\exists a \in \mathbb{Z}_m : a \cdot_m k = 1 &\iff (a \cdot k) \bmod m = 1 \\ &\iff \exists j \in \mathbb{Z} : a \cdot k = m \cdot j + 1 \\ &\iff a \cdot k - m \cdot j = 1\end{aligned}$$

L71: key lemma

Goal: $\forall m, m' \in \mathbb{N} \land n \in \mathbb{Z}^+ \land m \equiv m' \pmod{n} : \mathrm{CD}(m, n) = \mathrm{CD}(m', n)$

Assume:

1. $m, m' \in \mathbb{N} \land n \in \mathbb{Z}^+$
2. $m \equiv m' \pmod{n}$

$$m' = m + q \cdot n$$

$$\begin{aligned} d|m \land d|n &\implies d|(m + q \cdot n) \\ &\implies d|m' \land d|n \end{aligned}$$

Same for reverse.

L73: Euclid's algorithm for all divisors

Goal: For all positive m and n:

$$\mathrm{CD}(m, n) = \begin{cases} \mathrm{D}(n) & \text{if } n|m \\ \mathrm{CD}(n, \mathrm{rem}(m, n)) & \text{otherwise} \end{cases}$$

Case $n|m$

$d|n \iff d|m \land d|n$

Otherwise

Special case of (L71: key lemma)

P75: uniqueness of gcd

Goal: $\forall m, n, a, b \in \mathbb{N} : (\mathrm{CD}(m, n) = \mathrm{D}(a) \land \mathrm{CD}(m, n) = \mathrm{D}(b) \implies a = b)$

Assume:

1. $m, n, a, b \in \mathbb{N}$
2. $\mathrm{CD}(m, n) = \mathrm{D}(a) \land \mathrm{CD}(m, n) = \mathrm{D}(b)$

$$\begin{aligned} \mathrm{D}(a) = \mathrm{D}(b) &\implies a|b \land b|a \\ &\implies a = b \end{aligned}$$

P76: definition of gcd

Goal: the two statements are equivalent

- $\mathrm{CD}(m, n) = \mathrm{D}(k)$
- $k|m \land k|n \land (\forall d \in \mathbb{N} : d|m \land d|n \implies d|k)$

Assume:

1. $\mathrm{CD}(m, n) = \mathrm{D}(k)$

$$\begin{aligned} k \in \mathrm{CD}(m, n) &\implies k|m \land k|n \\ d|m \land d|n &\implies d \in \mathrm{D}(k) \implies d|k \end{aligned}$$

Assume:

1. $k|m \land k|n \land (\forall d \in \mathbb{N} : d|m \land d|n \implies d|k)$

$$\begin{aligned} d \in \mathrm{CD}(m, n) &\implies d \in \mathrm{D}(k) \\ d|k &\implies d|m \land d|n \quad \text{by transitivity} \\ &\implies d \in \mathrm{CD}(m, n) \end{aligned}$$

T78: Euclid’s algorithm gives the gcd

Goal: $\forall m, n \in \mathbb{Z}^+$: gcd terminates, and

- $\gcd(m, n) | m \land \gcd(m, n) | n$
- $\forall d \in \mathbb{Z} : d | m \land d | n \Longrightarrow d | \gcd(m, n)$

Assume:

1. $m, n \in \mathbb{Z}^+$

r decreases in natural numbers, this cannot continue forever, so gcd must terminate.

Euclid’s algorithm selects the greatest element of $\mathrm{CD}(m, n)$

$$\mathrm{CD}(m, n) = D(\gcd(m, n))$$

The two statements become trivial.

L80: properties of gcds

Goal: commutativity

$$\begin{aligned} \mathrm{D}(\gcd(m, n)) &= \mathrm{CD}(m, n) \\ &= \mathrm{D}(\gcd(n, m)) \\ \therefore \gcd(m, n) &= \gcd(n, m) \end{aligned}$$

Goal: associativity

Let $d_1 = \gcd(l, \gcd(m, n))$ and $d_2 = \gcd(\gcd(l, m), n)$

$$\begin{aligned} d_1 | \gcd(l, \gcd(m, n)) &\Longrightarrow d_1 | l \land d_1 | \gcd(m, n) \\ &\Longrightarrow d_1 | l \land d_1 | m \land d_1 | n \\ &\Longrightarrow d_1 | \gcd(l, m) \land d_1 | n \\ &\Longrightarrow d_1 | d_2 \end{aligned}$$

By same process, show $d_2 | d_1$ so $d_1 = d_2$

Goal: linearity

Let $d_1 = \gcd(l \cdot m, l \cdot n)$ and $d_2 = l \cdot \gcd(m, n)$

$$\begin{aligned} d_1 | \gcd(l \cdot m, l \cdot n) &\Longrightarrow d_1 | (l \cdot m) \land d_1 | (l \cdot n) \\ &\Longrightarrow {d_1}' | m \land {d_1}' | n \text{ where } d_1 = {d_1}' \cdot l \\ &\Longrightarrow {d_1}' | \gcd(m, n) \\ &\Longrightarrow d_1 | d_2 \\ d_2 | (l \cdot \gcd(m, n)) &\Longrightarrow {d_2}' | \gcd(m, n) \text{ where } d_2 = {d_2}' \cdot l \\ &\Longrightarrow \vdots \quad \text{same steps in reverse} \\ &\Longrightarrow d_2 | d_1 \\ \therefore d_1 &= d_2 \end{aligned}$$

T82: divisiblity of product with coprime factor

Goal: $\forall k, m, l \in \mathbb{Z}^+ : k | (m \cdot n) \land \gcd(k, m) = 1 \Longrightarrow k | n$

Assume:

1. $k, m, l \in \mathbb{Z}^+$
2. $k|(m \cdot n) \land \gcd(k, m) = 1$

$$\begin{aligned} k|(m \cdot n) &\implies k|\gcd(k \cdot n, m \cdot n) \\ &\implies k|(n \cdot \gcd(k, m))) \\ &\implies k|n \end{aligned}$$

C83: Euclid’s theorem

Goal: $\forall m, n \in \mathbb{Z}^+ \land p \text{ prime} : (p|(m \cdot n) \implies p|m \lor p|n)$

Assume:
1. $m, n \in \mathbb{Z}^+ \land p$ prime
2. $p|(m \cdot n)$

Case $p|m$

Goal closed.

Case $p \nmid m$

$\gcd(m, n) = 1 \implies p|n$

C85: inverse of modular integers

Goal: $\forall p$ prime, $i \in \mathbb{Z}_p : \left(i \neq 0 \implies [i^{p-2}]_m \cdot_m i = 1\right)$

Assume:
1. p prime, $i \in \mathbb{Z}_p$
2. $i \neq 0$

$$i^{p-1} \equiv 1 \pmod{p} \text{ by Fermat's little theorem } : p \text{ prime} \land p \nmid i$$

T87: gcd is a linear combination

We have the **extended Euclid algorithm** for writing gcd as a linear combination.