

### P8: product of odd integers

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

Assume:

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

$$m = 2a + 1$$

$$n = 2b + 1$$

$$m \cdot n = 2(2ab + a + b) + 1$$

### P10: rational square root

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

Assume:

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

$$\sqrt{x} = \frac{p}{q}$$

$$x = \frac{p^2}{q^2}$$

### T11: transitivity of implication

Goal:  $\forall P_1, P_2, P_3 : ((P_1 \implies P_2) \wedge (P_2 \implies P_3) \implies (P_1 \implies P_3))$

Assume:

1.  $P_1 \implies P_2$
2.  $P_2 \implies P_3$
3.  $P_1$

$$\implies P_2 \text{ by (1)}$$

$$\implies P_3 \text{ by (2)}$$

### P18: linearity of congruence

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

Assume:

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

$$a \equiv b \pmod{m} \iff a - b = k \cdot m$$

$$\iff n \cdot a - n \cdot b = k \cdot n \cdot m$$

$$\iff n \cdot a \equiv n \cdot b \pmod{n \cdot m}$$

### T19: 6 divisible

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

Assume:

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

$$6|n \implies n = 6k$$

$$\implies n = 3 \cdot (2k) \wedge n = 2 \cdot (3k)$$

$$\implies 3|n \wedge 2|n$$

$$n = 2a$$

$$n = 3b$$

$$3n = 6a$$

$$2n = 6b$$

$$n = 6(a - b)$$

$$\implies 6|n$$

### P21

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

Assume:

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

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

### T23: transitivity of divisibility

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

Assume:

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

$$m = a \cdot l$$

$$n = b \cdot m$$

$$n = (a \cdot b) \cdot l$$

$$\implies l|n$$

### T24: uniqueness of congruence

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

Assume:

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

#### Missing

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

Assume:

1.  $0 \leq z < m \wedge z \equiv n \pmod{m}$

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

$$z \equiv z' \pmod{m}$$

$$\implies z - z' = k \cdot m$$

$$-m < z - z' < m$$

$$\implies k = 0$$

$$\implies z = z'$$

### P25: square modulo 4

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

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:  $\forall p \in \mathbb{Z}^+ \wedge m \in \mathbb{N} : \left( m = 0 \vee m = p \implies \binom{p}{m} \equiv 1 \pmod{p} \right)$

Assume:

1.  $p \in \mathbb{Z}^+ \wedge m \in \mathbb{N}$

Case:  $m = 0$

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

Case:  $m = p$

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

**L28: non-ends of combinations**

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

Assume:

1.  $p \text{ prime} \wedge m \in \mathbb{Z}$
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:  $\forall p \text{ prime} \wedge m \in \mathbb{Z} \wedge 0 \leq m \leq p : \left( \binom{p}{m} \equiv 0 \pmod{p} \vee \binom{p}{m} \equiv 1 \pmod{p} \right)$

Assume:

1.  $p \text{ prime} \wedge m \in \mathbb{Z}$
2.  $0 \leq m \leq p$

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

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

Case  $0 < m < p$

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

**C33: the freshman's dream**

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

Assume:

1.  $m, n \in \mathbb{N} \wedge p \text{ prime}$

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

### C34: the dropout lemma

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

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

### C35: the many dropout lemma

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

Assume:

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

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

### T36: Fermat's little theorem (clause 1)

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

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

### T36: Fermat's little theorem (clause 2)

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

Assume:

1.  $i \in \mathbb{N} \wedge p \text{ prime} \wedge p \nmid i$

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

### C40: the contrapositive

Goal:  $(P \implies Q) \iff (\neg Q \implies \neg P)$

Assume:

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

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

Assume:

1.  $\neg Q \implies \neg P$
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:  $x \in \mathbb{Q} \iff \exists m, n \in \mathbb{Z}^+ : x = m/n \wedge \neg(\exists p \text{ prime} : p|m \wedge p|n)$

Assume:

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

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

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

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

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

Assume:

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

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

### 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  $r_0 < n \wedge m = q_0 \cdot m + r_0$

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 q0 r0`

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

$$k = q_k \cdot m + r_k$$

$$l = q_l \cdot m + r_l$$

$$\implies r_k \equiv r_l \pmod{m}$$

$$\implies r_k - r_l = a \cdot m$$

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

$$n = q \cdot m + \text{rem}(n, m)$$

$$\implies n - \text{rem}(n, m) = q \cdot m$$

$$\implies n \equiv \text{rem}(n, m) \pmod{m}$$

### 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:

$$-m < [k]_m - [k]_m' < m$$

$$[k]_m \equiv [k]_m' \pmod{m}$$

$$\implies [k]_m = [k]_m'$$

### 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:  $\forall m, m' \in \mathbb{N} \wedge n \in \mathbb{Z}^+ \wedge m \equiv m' \pmod{n} : \text{CD}(m, n) = \text{CD}(m', n)$

Assume:

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

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

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

Same for reverse.

### L73: Euclid's algorithm for all divisors

Goal: For all positive  $m$  and  $n$ :

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

Case  $n|m$

$$d|n \iff d|m \wedge d|n$$

Otherwise

Special case of (L71: key lemma)

### P75: uniqueness of gcd

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

Assume:

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

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

### P76: definition of gcd

Goal: the two statements are equivalent

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

Assume:

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

$$k \in \text{CD}(m, n) \implies k|m \wedge k|n$$

$$d|m \wedge d|n \implies d \in \text{D}(k) \implies d|k$$

Assume:

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

$$d \in \text{CD}(m, n) \implies d \in \text{D}(k)$$

$$d|k \implies d|m \wedge d|n \quad \text{by transitivity}$$

$$\implies d \in \text{CD}(m, n)$$

### T78: Euclid's algorithm gives the gcd

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

- $\text{gcd}(m, n) | m \wedge \text{gcd}(m, n) | n$
- $\forall d \in \mathbb{Z} : d | m \wedge d | n \implies d | \text{gcd}(m, n)$

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  $\text{CD}(m, n)$

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

The two statements become trivial.

### L80: properties of gcds

Goal: commutativity

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

Goal: associativity

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

$$\begin{aligned} d_1 | \text{gcd}(l, \text{gcd}(m, n)) &\implies d_1 | l \wedge d_1 | \text{gcd}(m, n) \\ &\implies d_1 | l \wedge d_1 | m \wedge d_1 | n \\ &\implies d_1 | \text{gcd}(l, m) \wedge d_1 | n \\ &\implies d_1 | d_2 \end{aligned}$$

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

Goal: linearity

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

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

### T82: divisibility of product with coprime factor

Goal:  $\forall k, m, n \in \mathbb{Z}^+ : k | (m \cdot n) \wedge \text{gcd}(k, m) = 1 \implies k | n$

Assume:



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

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

### C83: Euclid's theorem

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

Assume:

1.  $m, n \in \mathbb{Z}^+ \wedge p \text{ prime}$
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:  $\forall p \text{ prime}, i \in \mathbb{Z}_p : (i \neq 0 \implies [i^{p-2}]_m \cdot_m i = 1)$

Assume:

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

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

### T87: gcd is a linear combination

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

### P95: every positive integer $\geq 2$ is a product of primes

- $P(2)$  : trivial
- Assume  $\forall k < n : P(k)$ 
  - Then  $k$  is either a prime, or
  - A product of two numbers  $< k$ , the two numbers are products of primes.

### T96: fundamental theorem of arithmetic

Goal:  $\forall n \in \mathbb{Z}^+ : \text{there is a unique finite ordered sequence of primes such that}$

$$n = p_1 p_2 \dots p_l$$

Product of  $m$  primes  $\geq 2^m$ , if  $m$  is not finite then  $n$  is not finite.

Let  $p_1 p_2 \dots p_l$  and  $q_1 q_2 \dots q_k$  be product of primes equal to  $n$

- $p_1 | q_1 q_2 \dots q_k$ , name  $q_1$  to be the element equal to  $p_1$  so  $p_2 p_3 \dots p_l = q_2 q_3 \dots q_k = n/p_1$
- $p_2 | q_2 q_3 \dots q_k \implies p_2 = q_2, \dots$
- $q_{l+1} \dots q_k = 1$

$$\therefore l = k \text{ and } \forall i : p_i = q_i$$

### T99: set of primes is infinite

Suppose the set of primes  $\{p_1, p_2, \dots, p_n\}$  is finite

- Let  $p_m$  be the largest element

- $p_1 p_2 \dots p_n + 1$  is a prime and  $> p_m$ , contradiction.

### L103: properties of set relations

$\forall A, B, C$  sets

- Reflexivity:  $A \subseteq A$
- Transitivity:  $A \subseteq B \wedge B \subseteq C \implies A \subseteq C$
- Antisymmetry:  $A \subseteq B \wedge B \subseteq A \implies A = B$

Trivial

### P104: cardinality of the powerset

Goal:  $\forall U$  finite set :  $\#\mathcal{P}(U) = 2^{\#U}$

Let  $P(n) : \#U_n = n \implies \#\mathcal{P}(U_n) = 2^{\#U_n}$

- $P(0)$  : trivial
- Assume  $P(k)$ 
  - $\mathcal{P}(U_{k+1}) = \mathcal{P}(U_k) \cup \{\{x_{k+1}\} \cup A \mid A \in \mathcal{P}(U_k)\}$
  - $\#\mathcal{P}(U_{k+1}) = 2 \cdot \#\mathcal{P}(U_k) = 2^{\#U_{k+1}}$

### P105: subset of unions and intersections

Goal:  $\forall X \in \mathcal{P}(U) : (A \cup B \subseteq X \iff A \subseteq X \wedge B \subseteq X)$

Assume:

1.  $X \in \mathcal{P}(U)$

2.  $A \cup B \subseteq X$

$x \in A \implies x \in A \cup B \implies x \in X$   
 $x \in B \implies x \in A \cup B \implies x \in X$

2.  $A \subseteq X \wedge B \subseteq X$

3.  $x \in A \cup B$

Case  $x \in A \implies x \in X$

Case  $x \in B \implies x \in X$

Goal:  $\forall X \in \mathcal{P}(U) : (X \subseteq A \cap B \iff X \subseteq A \wedge X \subseteq B)$

Assume:

1.  $X \in \mathcal{P}(U)$

2.  $X \subseteq A \cap B$

$x \in X \implies x \in A \cap B \implies x \in A$   
 $x \in X \implies x \in A \cap B \implies x \in B$

2.  $X \subseteq A \wedge X \subseteq B$

$x \in X \implies x \in A \wedge x \in B \implies x \in A \cap B$

### C106: set equality with unions and intersections (clause 1)

Let  $A, B, C \in \mathcal{P}(U)$

Goal:  $C = A \cup B$  iff

- $A \subseteq C \wedge B \subseteq C$
- $\forall X \in \mathcal{P}(U) : (A \subseteq X \wedge B \subseteq X \implies C \subseteq X)$

Assume:

1.  $C \subseteq A \cup B$

$A \subseteq C \wedge B \subseteq C$  by (P105)

Assume:

1.  $X \in \mathcal{P}(U) \wedge A \subseteq X \wedge B \subseteq X$

$C = A \cup B \subseteq X$  by (P105)

Assume:

1.  $A \subseteq C \wedge B \subseteq C$
2.  $\forall X \in \mathcal{P}(U) : (A \subseteq X \wedge B \subseteq X \implies C \subseteq X)$

$A \cup B \subseteq C$  by (1) and (P105)

$C \subseteq A \cup B$  by (2) and (P105)

$\implies A \cup B = C$

### C106: set equality with unions and intersections (clause 2)

Goal:  $C = A \cap B$  iff

- $C \subseteq A \wedge C \subseteq B$
- $\forall X \in \mathcal{P}(U) : (X \subseteq A \wedge X \subseteq B \implies X \subseteq C)$

The proof is exactly the same as clause 1.

### P107: results from singleton and pair set equalities

Goal:  $\{x, y\} \subseteq \{a\} \implies x = y = a$

$$x \in \{x, y\} \implies x \in \{a\} \implies x = a$$

Same for  $y$

Goal:  $\{c, x\} = \{c, y\} \implies x = y$

Case  $x = c$

$y = c$  by previous goal.

Case  $x \neq c$

$$x \in \{c, y\} \implies x = c \vee x = y \implies x = y$$

### P108: fundamental property of ordered pairing

Let  $\langle a, b \rangle = \{\{a\}, \{a, b\}\}$

Goal:  $\langle a, b \rangle = \langle x, y \rangle \implies a = x \wedge b = y$

Case  $a = b$

$$\langle a, b \rangle = \{\{a\}\} = \langle x, y \rangle$$

Case  $a \neq b$

$$\{x\} \in \{\{a\}, \{a, b\}\} \implies \{x\} = \{a\} \implies x = a$$

$$\{a, b\} \in \{a, \{a, y\}\} \implies \{a, b\} = \{a, y\} \implies b = y$$

### P110: cardinality of cartesian products

Goal:  $\#(A \times B) = \#A \cdot \#B$

Let  $P(n) : \#B_n = n \implies \#(A \times B_n) = \#A \cdot \#B_n$

- $P(1)$  : trivial
- Assume  $P(k)$

$$A \times B_{k+1} = A \times B_k \cup A \times \{b_{k+1}\}$$

$$\#(A \times B_{k+1}) = \#A \cdot \#B_k + \#A = \#A \cdot \#B_{k+1}$$