# Formal Proofs on Congruences

## Transitivity

Let $a$, $b$, and $m$ be non-negative integers with $m \neq 0$.
Prove that, if $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

| | | |
|---|---|---|
| 1.1. | $\mathsf{Congruent}(a, b, m) \wedge \mathsf{Congruent}(b, c, m)$ | Assumption |
| 1.2. | $\mathsf{Congruent}(a, b, m)$ | Elim $\wedge$: 1.1 |
| 1.3. | $\mathsf{Congruent}(b, c, m)$ | Elim $\wedge$: 1.1 |
| 1.4. | $\mathsf{Divides}(m, a - b)$ | Def of Congruent: 1.2 |
| 1.5. | $\mathsf{Divides}(m, b - c)$ | Def of Congruent: 1.3 |
| 1.6. | $\exists\, k, a - b = k\, m$ | Def of Divides: 1.4 |
| 1.7. | $\exists\, k, b - c = k\, m$ | Def of Divides: 1.5 |
| 1.8. | $a - b = s\, m$ | Elim $\exists$: 1.6 |
| 1.9. | $b - c = t\, m$ | Elim $\exists$: 1.7 |
| 1.10. | $a - c = (s + t)\, m$ | Algebra: 1.8 1.9 |
| 1.11. | $\exists\, k, a - c = k\, m$ | Intro $\exists$: 1.10 |
| 1.12. | $\mathsf{Divides}(m, a - c)$ | Undef Divides: 1.11 |
| 1.13. | $\mathsf{Congruent}(a, c, m)$ | Undef Congruent: 1.12 |
| 1. | $\mathsf{Congruent}(a, b, m) \wedge \mathsf{Congruent}(b, c, m) \rightarrow \mathsf{Congruent}(a, c, m)$ | Direct Proof |

**English**: Suppose that $a \equiv_m b$ and $c \equiv_m d$. Unrolling the definitions, we have $a - b = sm$ and $b - c = tm$ for some integers $s$, $t$. Adding these two equations, we see that $a - c = (a - b) + (b - c) = sm + tm = (s + t)m$. This shows that $a \equiv_m c$ by definition.

## Congruence From Equation

Let $a$, $b$, and $m$ be non-negative integers with $m \neq 0$.
Prove that, if $a = b$, then $a \equiv_m b$.

| | | |
|---|---|---|
| 1.1. | $a = b$ | Assumption |
| 1.2. | $a - b = 0\,m$ | Algebra: 1.1 |
| 1.3. | $\exists\, k, a - b = k\,m$ | Intro ∃: 1.2 |
| 1.4. | $\mathsf{Divides}(m, a - b)$ | Undef Divides: 1.3 |
| 1.5. | $\mathsf{Congruent}(a, b, m)$ | Undef Congruent: 1.4 |
| 1. | $a = b \to \mathsf{Congruent}(a, b, m)$ | Direct Proof |

**English**: Suppose that $a = b$. This tells us that $a - b = 0 = 0 \cdot m$, showing $a \equiv_m b$, by definition.

## Adding Congruences

Let $a$, $b$, $c$, $d$, and $m$ be non-negative integers with $m \neq 0$.
Prove that, if $a \equiv_m b$ and $c \equiv_m d$, then $a + b \equiv_m c + d$.

| | | |
|---|---|---|
| 1.1. | $\mathsf{Congruent}(a, b, m) \wedge \mathsf{Congruent}(c, d, m)$ | Assumption |
| 1.2. | $\mathsf{Congruent}(a, b, m)$ | Elim ∧: 1.1 |
| 1.3. | $\mathsf{Congruent}(c, d, m)$ | Elim ∧: 1.1 |
| 1.4. | $\mathsf{Divides}(m, a - b)$ | Def of Congruent: 1.2 |
| 1.5. | $\mathsf{Divides}(m, c - d)$ | Def of Congruent: 1.3 |
| 1.6. | $\exists\, k, a - b = k\,m$ | Def of Divides: 1.4 |
| 1.7. | $\exists\, k, c - d = k\,m$ | Def of Divides: 1.5 |
| 1.8. | $a - b = s\,m$ | Elim ∃: 1.6 |
| 1.9. | $c - d = t\,m$ | Elim ∃: 1.7 |
| 1.10. | $a + c - b + d = (s + t)\,m$ | Algebra: 1.8 1.9 |
| 1.11. | $\exists\, k, a + c - b + d = k\,m$ | Intro ∃: 1.10 |
| 1.12. | $\mathsf{Divides}(m, a + c - b + d)$ | Undef Divides: 1.11 |
| 1.13. | $\mathsf{Congruent}(a + c, b + d, m)$ | Undef Congruent: 1.12 |
| 1. | $\mathsf{Congruent}(a, b, m) \wedge \mathsf{Congruent}(c, d, m) \to \mathsf{Congruent}(a + c, b + d, m)$ | Direct Proof |

**English**: Suppose that $a \equiv_m b$ and $c \equiv_m d$. Unrolling the definitions, we have $a - b = sm$ and $c - d = tm$ for some integers $s$ and $t$. Adding these two equations, we see that $(a + c) - (b + d) = (a - b) + (c - d) = sm + tm = (s + t)m$. This shows that $a + c \equiv_m b + d$ by definition.

## Multiplying Congruences

Let $a$, $b$, $c$, $d$, and $m$ be non-negative integers with $m \neq 0$.
Prove that, if $a \equiv_m b$ and $c \equiv_m d$, then $ab \equiv_m cd$.

In doing this proof formally, we will need to apply a theorem for multiplying equations. It says

$$\text{MultEqns:} \quad \forall a\, \forall b\, \forall c\, \forall d\, ((a = b \wedge c = d) \rightarrow (ac = bd))$$

| | | |
|---|---|---|
| 1.1. | $\mathsf{Congruent}(a, b, m) \wedge \mathsf{Congruent}(c, d, m)$ | Assumption |
| 1.2. | $\mathsf{Congruent}(a, b, m)$ | Elim $\wedge$: 1.1 |
| 1.3. | $\mathsf{Congruent}(c, d, m)$ | Elim $\wedge$: 1.1 |
| 1.4. | $\mathsf{Divides}(m, a - b)$ | Def of Congruent: 1.2 |
| 1.5. | $\mathsf{Divides}(m, c - d)$ | Def of Congruent: 1.3 |
| 1.6. | $\exists\, k, a - b = k\, m$ | Def of Divides: 1.4 |
| 1.7. | $\exists\, k, c - d = k\, m$ | Def of Divides: 1.5 |
| 1.8. | $a - b = s\, m$ | Elim $\exists$: 1.6 |
| 1.9. | $c - d = t\, m$ | Elim $\exists$: 1.7 |
| 1.10. | $a = b + s\, m$ | Algebra: 1.8 |
| 1.11. | $c = d + t\, m$ | Algebra: 1.9 |
| 1.12. | $a = b + s\, m \wedge c = d + t\, m$ | Intro $\wedge$: 1.10, 1.11 |
| 1.13. | $a\, c = (b + s\, m)\, (d + t\, m)$ | Apply MultEqns: 1.12 |
| 1.14. | $a\, c - b\, d = (b\, t + d\, s + s\, t\, m)\, m$ | Algebra: 1.13 |
| 1.15. | $\exists\, k, a\, c - b\, d = k\, m$ | Intro $\exists$: 1.14 |
| 1.16. | $\mathsf{Divides}(m, a\, c - b\, d)$ | Undef Divides: 1.15 |
| 1.17. | $\mathsf{Congruent}(a\, c, b\, d, m)$ | Undef Congruent: 1.16 |
| 1. | $\mathsf{Congruent}(a, b, m) \wedge \mathsf{Congruent}(c, d, m) \rightarrow \mathsf{Congruent}(a\, c, b\, d, m)$ | Direct Proof |

**English**: Suppose that $a \equiv_m b$ and $c \equiv_m d$. Unrolling the definitions, we have $a - b = sm$ and $c - d = tm$ for some integers $s$ and $t$. We can write these equivalently as $a = b + sm$ and $c = d + tm$. Multiplying these last two equations, we see that $ac = (b + sm)(d + tm) = bd + (bt + sd + stm)m$. This last equation can be rewritten $ac - bd = (bt + sd + stm)m$, which shows that $ac \equiv_m bd$.

# Modular Arithmetic: A Property

Let $a$, $b$, and $m$ be non-negative integers with $0 < m$.
Prove that $a \equiv_m b$ iff $a \bmod m = b \bmod m$.

This proof is longer, so we will split it into parts. We will prove each implication separately:

Lemma 1.1: $\forall a \, \forall b \, \forall m \, (0 < m \rightarrow \mathsf{mod}(a, m) = \mathsf{mod}(b, m) \rightarrow \mathsf{Congruent}(a, b, m))$
Lemma 1.2: $\forall a \, \forall b \, \forall m \, (0 < m \rightarrow \mathsf{Congruent}(a, b, m) \rightarrow \mathsf{mod}(a, m) = \mathsf{mod}(b, m))$

With those in hand, we prove this as follows. (Try it yourself here.)

| | | |
|---|---|---|
| 1. | $0 < m$ | Given |
| 2. | $\mathsf{mod}(a, m) = \mathsf{mod}(b, m) \rightarrow \mathsf{Congruent}(a, b, m)$ | Apply Lemma1_1: 1 |
| 3. | $\mathsf{Congruent}(a, b, m) \rightarrow \mathsf{mod}(a, m) = \mathsf{mod}(b, m)$ | Apply Lemma1_2: 1 |
| 4. | $(\mathsf{mod}(a, m) = \mathsf{mod}(b, m) \rightarrow \mathsf{Congruent}(a, b, m)) \land$ $(\mathsf{Congruent}(a, b, m) \rightarrow \mathsf{mod}(a, m) = \mathsf{mod}(b, m))$ | Intro $\land$: 2, 3 |
| 5. | $\mathsf{Congruent}(a, b, m) \leftrightarrow \mathsf{mod}(a, m) = \mathsf{mod}(b, m)$ | Equivalent: 4 |

Now, we can move on to proving the two lemmas we used above...

## Lemma 1.1

Prove that $a \bmod m = b \bmod m$ implies $a \equiv_m b$.

| | | |
|---|---|---|
| 1. | $0 < m$ | Given |
| 2. | $a = \mathsf{div}(a, m)\, m + \mathsf{mod}(a, m) \land 0 \leq \mathsf{mod}(a, m) \land \mathsf{mod}(a, m) < m$ | Apply Division: 1 |
| 3. | $b = \mathsf{div}(b, m)\, m + \mathsf{mod}(b, m) \land 0 \leq \mathsf{mod}(b, m) \land \mathsf{mod}(b, m) < m$ | Apply Division: 1 |
| 4. | $a = \mathsf{div}(a, m)\, m + \mathsf{mod}(a, m) \land 0 \leq \mathsf{mod}(a, m)$ | Elim $\land$: 2 |
| 5. | $a = \mathsf{div}(a, m)\, m + \mathsf{mod}(a, m)$ | Elim $\land$: 4 |
| 6. | $b = \mathsf{div}(b, m)\, m + \mathsf{mod}(b, m) \land 0 \leq \mathsf{mod}(b, m)$ | Elim $\land$: 3 |
| 7. | $b = \mathsf{div}(b, m)\, m + \mathsf{mod}(b, m)$ | Elim $\land$: 6 |
| 8.1. | $\mathsf{mod}(a, m) = \mathsf{mod}(b, m)$ | Assumption |
| 8.2. | $a = \mathsf{div}(a, m)\, m + \mathsf{mod}(b, m)$ | Substitute: 8.1, 5 |
| 8.3. | $a - b = (\mathsf{div}(a, m) - \mathsf{div}(b, m))\, m$ | Algebra: 7 8.2 |
| 8.4. | $\exists\, k, a - b = k\, m$ | Intro $\exists$: 8.3 |
| 8.5. | $\mathsf{Divides}(m, a - b)$ | Undef Divides: 8.4 |
| 8.6. | $\mathsf{Congruent}(a, b, m)$ | Undef Congruent: 8.5 |
| 8. | $\mathsf{mod}(a, m) = \mathsf{mod}(b, m) \rightarrow \mathsf{Congruent}(a, b, m)$ | Direct Proof |

**English**: By the Division Theorem, we can write $a$ and $b$ in the form $a = \mathsf{div}(a, m)m + \mathsf{mod}(a, m)$ and $b = \mathsf{div}(b, m)m + \mathsf{mod}(b, m)$.

Now, suppose that $\mathsf{mod}(a, m) = \mathsf{mod}(b, m)$. Then, we can calculate

$$\begin{aligned} a - b &= (\mathsf{div}(a, m) - \mathsf{div}(b, m))\, m + (\mathsf{mod}(a, m) - \mathsf{mod}(b, M)) \\ &= (\mathsf{div}(a, m) - \mathsf{div}(b, m))\, m \end{aligned}$$

This shows that $m \mid a - b$, which means that $a \equiv_m b$, by definition.

### Lemma 1.2

Prove that $a \equiv_m b$ implies $a \bmod m = b \bmod m$.

In doing so, we will use the uniqueness property of the remainder, which says

$$\forall a\, \forall b\, \forall q\, \forall r\, (((a = qb + r) \wedge (0 \le r) \wedge (r < b)) \rightarrow (q = \mathsf{div}(a, b) \wedge r = \mathsf{mod}(a, b)))$$

| | |
|---|---|
| 1. $0 < m$ | Given |
| 2. $a = \mathsf{div}(a, m)\, m + \mathsf{mod}(a, m) \wedge 0 \le \mathsf{mod}(a, m) \wedge \mathsf{mod}(a, m) < m$ | Apply Division: 1 |
| 3. $b = \mathsf{div}(b, m)\, m + \mathsf{mod}(b, m) \wedge 0 \le \mathsf{mod}(b, m) \wedge \mathsf{mod}(b, m) < m$ | Apply Division: 1 |
| 4. $a = \mathsf{div}(a, m)\, m + \mathsf{mod}(a, m) \wedge 0 \le \mathsf{mod}(a, m)$ | Elim $\wedge$: 2 |
| 5. $b = \mathsf{div}(b, m)\, m + \mathsf{mod}(b, m) \wedge 0 \le \mathsf{mod}(b, m)$ | Elim $\wedge$: 3 |
| 6. $a = \mathsf{div}(a, m)\, m + \mathsf{mod}(a, m)$ | Elim $\wedge$: 4 |
| 7. $b = \mathsf{div}(b, m)\, m + \mathsf{mod}(b, m)$ | Elim $\wedge$: 5 |
| 8.1. $\mathsf{Congruent}(a, b, m)$ | Assumption |
| 8.2. $\mathsf{Divides}(m, a - b)$ | Def of Congruent: 8.1 |
| 8.3. $\exists\, k, a - b = k\, m$ | Def of Divides: 8.2 |
| 8.4. $a - b = k\, m$ | Elim $\exists$: 8.3 |
| 8.5. $b = (\mathsf{div}(a, m) - k)\, m + \mathsf{mod}(a, m)$ | Algebra: 6 7 8.4 |
| 8.6. $0 \le mod(a, m)$ | Elim $\wedge$: 4 |
| 8.7. $b = (\mathsf{div}(a, m) - k)\, m + \mathsf{mod}(a, m) \wedge 0 \le \mathsf{mod}(a, m)$ | Intro $\wedge$: 8.5, 8.6 |
| 8.8. $\mathsf{mod}(a, m) < m$ | Elim $\wedge$: 2 |
| 8.9. $b = (\mathsf{div}(a, m) - k)\, m + \mathsf{mod}(a, m) \wedge 0 \le \mathsf{mod}(a, m) \wedge mod(a, m) < m$ | Intro $\wedge$: 8.7, 8.8 |
| 8.10. $\mathsf{div}(a, m) - k = \mathsf{div}(b, m) \wedge \mathsf{mod}(a, m) = \mathsf{mod}(b, m)$ | Apply DivisionUnique: 8.9 |
| 8.11. $\mathsf{mod}(a, m) = \mathsf{mod}(b, m)$ | Elim $\wedge$: 8.10 |
| 8. $\mathsf{Congruent}(a, b, m) \rightarrow \mathsf{mod}(a, m) = \mathsf{mod}(b, m)$ | Direct Proof |

**English**: By the Division Theorem, we can write $a$ and $b$ in the form $a = \mathsf{div}(a, m)m + \mathsf{mod}(a, m)$ and $b = \mathsf{div}(b, m)m + \mathsf{mod}(b, m)$.

Now, suppose that $a \equiv_m b$. Unrolling the definitions, this says that $b = a - km$ for some integer $k$. Thus, we have

$$\begin{aligned} b &= \mathsf{div}(a, m)\, m + \mathsf{mod}(a, m) - km \\ &= (\mathsf{div}(a, m) - k)\, m + \mathsf{mod}(a, m) \end{aligned}$$

Since $0 \le \mathsf{div}(a, m) < m$, the Division Uniqueness Theorem says that $\mathsf{mod}(a, m) = \mathsf{mod}(b, m)$.

## Useful GCD Fact

Let $a$ and $b$ be positive integers.
Prove that $\gcd(a, b) = \gcd(b, a \bmod b)$.

This proof is long, so we will split it into parts. We will prove each implication separately:

Lemma 2.1: $\forall a\, \forall b\, \forall d\, (((d \mid a) \land (d \mid b)) \to ((d \mid b) \land (d \mid a \bmod b)))$
Lemma 2.2: $\forall a\, \forall b\, \forall d\, (((d \mid b) \land (d \mid a \bmod b)) \to ((d \mid a) \land (d \mid b)))$
Lemma 3: $\forall a\, \forall b\, \forall c\, \forall d\, (\forall x\, ((x \mid a) \land (x \mid b)) \to ((x \mid c) \land (x \mid d)) \to (\gcd(a, b) \leq \gcd(c, d)))$
Lemma 4: $\forall a\, \forall b\, (((a \leq b) \land (b \leq a)) \to (a = b))$

With those in hand, we prove this as follows.

| | | |
|---|---|---|
| 1. | $\forall\, a, \forall\, b, \forall\, d, \mathsf{Divides}(d, a) \land \mathsf{Divides}(d, b) \to \mathsf{Divides}(d, b) \land \mathsf{Divides}(d, \mathsf{mod}(a, b))$ | Cite Lemma2_1 |
| 2. | $\forall\, a, \forall\, b, \forall\, d, \mathsf{Divides}(d, b) \land \mathsf{Divides}(d, \mathsf{mod}(a, b)) \to \mathsf{Divides}(d, a) \land \mathsf{Divides}(d, b)$ | Cite Lemma2_2 |
| 3. | $\forall\, b, \forall\, d, \mathsf{Divides}(d, a) \land \mathsf{Divides}(d, b) \to \mathsf{Divides}(d, b) \land \mathsf{Divides}(d, \mathsf{mod}(a, b))$ | Elim $\forall$: 1 |
| 4. | $\forall\, b, \forall\, d, \mathsf{Divides}(d, b) \land \mathsf{Divides}(d, \mathsf{mod}(a, b)) \to \mathsf{Divides}(d, a) \land \mathsf{Divides}(d, b)$ | Elim $\forall$: 2 |
| 5. | $\forall\, d, \mathsf{Divides}(d, a) \land \mathsf{Divides}(d, b) \to \mathsf{Divides}(d, b) \land \mathsf{Divides}(d, \mathsf{mod}(a, b))$ | Elim $\forall$: 3 |
| 6. | $\forall\, d, \mathsf{Divides}(d, b) \land \mathsf{Divides}(d, \mathsf{mod}(a, b)) \to \mathsf{Divides}(d, a) \land \mathsf{Divides}(d, b)$ | Elim $\forall$: 4 |
| 7. | $\gcd(a, b) \leq \gcd(b, \mathsf{mod}(a, b))$ | Apply Lemma3: 5 |
| 8. | $\gcd(b, \mathsf{mod}(a, b)) \leq \gcd(a, b)$ | Apply Lemma3: 6 |
| 9. | $\gcd(a, b) \leq \gcd(b, \mathsf{mod}(a, b)) \land \gcd(b, \mathsf{mod}(a, b)) \leq \gcd(a, b)$ | Intro $\land$: 7, 8 |
| 10. | $\gcd(a, b) = \gcd(b, \mathsf{mod}(a, b))$ | Apply Lemma4: 9 |

**English**: Applying Lemma 3 to $a$, $b$, $b$, $a \bmod b$, its premise becomes Lemma 2.1, so we conclude that $\gcd(a, b) \leq \gcd(b, a \bmod b)$. Applying Lemma 3 to $b$, $a \bmod b$, $a$, $b$, its premise becomes Lemma 2.2, so we conclude that $\gcd(b, a \bmod b) \leq \gcd(a, b)$. Thus, by Lemma 4, we get $\gcd(a, b) = \gcd(b, a \bmod b)$.

## Lemma 2.1

Prove that $(d \mid b)$ and $(d \mid a \bmod b)$ follow from $d \mid a$ and $d \mid b$.

| | | |
|---|---|---|
| 1. | $\mathsf{Divides}(d, a)$ | Given |
| 2. | $\mathsf{Divides}(d, b)$ | Given |
| 3. | $0 < b$ | Given |
| 4. | $\exists\, k, a = k\, d$ | Def of Divides: 1 |
| 5. | $\exists\, k, b = k\, d$ | Def of Divides: 2 |
| 6. | $a = s\, d$ | Elim $\exists$: 4 |
| 7. | $b = t\, d$ | Elim $\exists$: 5 |
| 8. | $a = \mathsf{div}(a, b)\, b + \mathsf{mod}(a, b) \land 0 \leq \mathsf{mod}(a, b) \land \mathsf{mod}(a, b) < b$ | Apply Division: 3 |
| 9. | $a = \mathsf{div}(a, b)\, b + \mathsf{mod}(a, b) \land 0 \leq \mathsf{mod}(a, b)$ | Elim $\land$: 8 |
| 10. | $a = \mathsf{div}(a, b)\, b + \mathsf{mod}(a, b)$ | Elim $\land$: 9 |
| 11. | $s\, d = \mathsf{div}(s\, d, b)\, b + \mathsf{mod}(s\, d, b)$ | Substitute: 6, 10 |
| 12. | $s\, d = \mathsf{div}(s\, d, t\, d)\, t\, d + \mathsf{mod}(s\, d, t\, d)$ | Substitute: 7, 11 |
| 13. | $\mathsf{mod}(s\, d, t\, d) = (s - \mathsf{div}(s\, d, t\, d)\, t)\, d$ | Algebra: 12 |
| 14. | $\mathsf{mod}(a, t\, d) = (s - \mathsf{div}(a, t\, d)\, t)\, d$ | Substitute: 6, 13 |
| 15. | $\mathsf{mod}(a, b) = (s - \mathsf{div}(a, b)\, t)\, d$ | Substitute: 7, 14 |
| 16. | $\exists\, k, \mathsf{mod}(a, b) = k\, d$ | Intro $\exists$: 15 |
| 17. | $\mathsf{Divides}(d, \mathsf{mod}(a, b))$ | Undef Divides: 16 |
| 18. | $\mathsf{Divides}(d, b) \land \mathsf{Divides}(d, mod(a, b))$ | Intro $\land$: 2, 17 |

**English**: Since $d \mid a$, we know that $a = sd$, for some integer $s$, by the definition of divides. Likewise, since $d \mid b$, we know that $b = td$, for some integer $t$, by the definition of divides.

By the Division Theorem, we can write $a = qb + \mathsf{mod}(a, b)$. Solving for $\mathsf{mod}(a, b)$, we have $\mathsf{mod}(a, b) = a - qb$. Substituting in the prior facts about $a$ and $b$ and pulling out a common factor of $d$, we have $\mathsf{mod}(a, b) = (s - qt)d$. This shows that $d \mid \mathsf{mod}(a, b)$ by the definition of divides.

## Lemma 2.2

Prove that $(d \mid a)$ and $(d \mid b)$ follow from $d \mid b$ and $d \mid a \bmod b$.
(Note: you will need `substitute` as well as `algebra`.)

| | | |
|---|---|---|
| 1. | $\mathsf{Divides}(d, b)$ | Given |
| 2. | $\mathsf{Divides}(d, \mathsf{mod}(a, b))$ | Given |
| 3. | $0 < b$ | Given |
| 4. | $\exists\, k, b = k\, d$ | Def of Divides: 1 |
| 5. | $\exists\, k, \mathsf{mod}(a, b) = k\, d$ | Def of Divides: 2 |
| 6. | $b = s\, d$ | Elim $\exists$: 4 |
| 7. | $\mathsf{mod}(a, b) = t\, d$ | Elim $\exists$: 5 |
| 8. | $a = \mathsf{div}(a, b)\, b + \mathsf{mod}(a, b) \wedge 0 \leq \mathsf{mod}(a, b) \wedge \mathsf{mod}(a, b) < b$ | Apply Division: 3 |
| 9. | $a = \mathsf{div}(a, b)\, b + \mathsf{mod}(a, b) \wedge 0 \leq \mathsf{mod}(a, b)$ | Elim $\wedge$: 8 |
| 10. | $a = \mathsf{div}(a, b)\, b + \mathsf{mod}(a, b)$ | Elim $\wedge$: 9 |
| 11. | $a = \mathsf{div}(a, b)\, b + t\, d$ | Substitute: 7, 10 |
| 12. | $a = \mathsf{div}(a, s\, d)\, s\, d + t\, d$ | Substitute: 6, 11 |
| 13. | $a = (\mathsf{div}(a, s\, d)\, s + t)\, d$ | Algebra: 12 |
| 14. | $\exists\, k, a = k\, d$ | Intro $\exists$: 13 |
| 15. | $\mathsf{Divides}(d, a)$ | Undef Divides: 14 |
| 16. | $\mathsf{Divides}(d, a) \wedge \mathsf{Divides}(d, b)$ | Intro $\wedge$: 15, 1 |

**English**: Since $d \mid b$, we know that $b = sd$, for some integer $s$, by the definition of divides. Likewise, since $d \mid a \bmod b$, we know that $a \bmod b = td$, for some integer $t$.

By the Division Theorem, we can write $a = qb + \mathsf{mod}(a, b)$. Substituting in the prior facts above and pulling out a common factor of $d$, we have $a = (qs + t)d$. This shows that $d \mid a$ by definition.

## Lemma 3

Let $a$, $b$, $c$, and $d$ be positive integers.
Prove that $\gcd(a,b) \mid \gcd(c,d)$ follows from $\forall x\,(((x \mid a) \wedge (x \mid b)) \to ((x \mid c) \wedge (x \mid d)))$.

In order to do so, we will need the following two facts about GCD (the first is its definition):

$$\text{GCD Pos:}\ \ \forall a\,\forall b\,(\top \to (((\gcd(a,b) \mid a) \wedge (\gcd(a,b) \mid b)) \wedge \forall d\,(((d \mid a) \wedge d \mid b)) \to (d \mid \gcd(a,b)))))$$
$$\text{GCD Unique:}\ \ \forall a\,\forall b\,\forall x\,(((x \mid a) \wedge (x \mid b) \wedge \forall d\,(((d \mid a) \wedge (d \mid b)) \to (d \leq x))) \to (x = \gcd(a,b)))$$

The first fact has a (trivial) premise in order to make it easier to use with `apply`.

| | | |
|---|---|---|
| 1. | $\forall\, x, \mathsf{Divides}(x,a) \wedge \mathsf{Divides}(x,b) \to \mathsf{Divides}(x,c) \wedge \mathsf{Divides}(x,d)$ | Given |
| 2. | $\top$ | Ad Litteram Verum |
| 3. | $\mathsf{Divides}(\gcd(a,b),a) \wedge \mathsf{Divides}(\gcd(a,b),b) \wedge (\forall\, d, \mathsf{Divides}(d,a) \wedge \mathsf{Divides}(d,b) \to d \leq \gcd(a,b))$ | Apply GCDPos: 2 |
| 4. | $\mathsf{Divides}(\gcd(c,d),c) \wedge \mathsf{Divides}(\gcd(c,d),d) \wedge (\forall\, d0, \mathsf{Divides}(d0,c) \wedge \mathsf{Divides}(d0,d) \to d0 \leq \gcd(c,d))$ | Apply GCDPos: 2 |
| 5. | $\mathsf{Divides}(\gcd(a,b),a) \wedge \mathsf{Divides}(\gcd(a,b),b)$ | Elim ∧: 3 |
| 6. | $\mathsf{Divides}(\gcd(a,b),a) \wedge \mathsf{Divides}(\gcd(a,b),b) \to \mathsf{Divides}(\gcd(a,b),c) \wedge \mathsf{Divides}(\gcd(a,b),d)$ | Elim ∀: 1 |
| 7. | $\mathsf{Divides}(\gcd(a,b),c) \wedge \mathsf{Divides}(\gcd(a,b),d)$ | Modus Ponens: 5, 6 |
| 8. | $\forall\, d0, \mathsf{Divides}(d0,c) \wedge \mathsf{Divides}(d0,d) \to d0 \leq \gcd(c,d)$ | Elim ∧: 4 |
| 9. | $\mathsf{Divides}(\gcd(a,b),c) \wedge \mathsf{Divides}(\gcd(a,b),d) \to \gcd(a,b) \leq \gcd(c,d)$ | Elim ∀: 8 |
| 10. | $\gcd(a,b) \leq \gcd(c,d)$ | Modus Ponens: 7, 9 |

**English**: By GCD Pos, we know that $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$. We are given that anything that divides $a$ and $b$ also divides $c$ and $d$. Applying that to $\gcd(a,b)$, we get that $\gcd(a,b) \mid c$ and $\gcd(a,b) \mid d$. By GCD Pos, any positive integer with the latter two properties is no bigger than $\gcd(c,d)$. Applying that to $\gcd(a,b)$, we get that $\gcd(a,b) \leq \gcd(c,d)$.

## Lemma 4

Let $a$ and $b$ be positive integers.
Prove that $a = b$ follows from $a \leq b$ and $b \leq a$.

In order to do so, we will need the following facts about "$\leq$" and "$<$":

$$\text{LessOrEqual: } \forall a\, \forall b\, ((a \leq b) \rightarrow ((a = b) \vee (a < b)))$$
$$\text{LessVsGreater: } \forall a\, \forall b\, ((a < b) \rightarrow \neg(b < a))$$

The first fact is the definition of "$\leq$". The says that "$<$" is anti-symmetric.
(Hint: Prove it by cases over $a < b$ and $\neg(a < b)$.)

| | | |
|---|---|---|
| 1. | $a \leq b$ | Given |
| 2. | $b \leq a$ | Given |
| 3. | $a = b \vee a < b$ | Apply LessOrEqual: 1 |
| 4. | $b = a \vee b < a$ | Apply LessOrEqual: 2 |
| 5.1. | $a < b$ | Assumption |
| 5.2. | $\neg(b < a)$ | Apply LessVsGreater: 5.1 |
| 5.3. | $b = a$ | Elim $\vee$: 4, 5.2 |
| 5.4. | $a = b$ | Algebra: 5.3 |
| 5. | $a < b \rightarrow a = b$ | Direct Proof |
| 6.1. | $\neg(a < b)$ | Assumption |
| 6.2. | $a = b$ | Elim $\vee$: 3, 6.1 |
| 6. | $\neg(a < b) \rightarrow a = b$ | Direct Proof |
| 7. | $a = b$ | Simple Cases: 5, 6 |

**English**: We will prove this by cases over whether $a < b$ or $\neg(a < b)$.

Suppose that $\neg(a < b)$. Since $a \leq b$, we must have $a = b$, by the definition of "$\leq$".

Now, suppose that $a < b$. This means that $\neg(b < a)$ by the anti-symmetry of "$<$". Since $b \leq a$, we must have $b = a$, by the definition of '$\leq$", which can be rewritten $a = b$.