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 $a \equiv_m c$.

Formal: Try it yourself here.

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 $a \equiv_m b$.

Formal: Try it yourself here.

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 $a + b \equiv_m c + d$.

Formal: Try it yourself here.

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

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

Formal: Try it yourself here.

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: $\forall a\, \forall b\, \forall m\, (0 < m \to \mathsf{mod}(a, m) = \mathsf{mod}(b, m) \to \mathsf{Congruent}(a, b, m))$

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

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

1.	$0 < m$	Given
2.	$\mathsf{mod}(a, m) = \mathsf{mod}(b, m) \to \mathsf{Congruent}(a, b, m)$	Apply Lemma1_1: 1
3.	$\mathsf{Congruent}(a, b, m) \to \mathsf{mod}(a, m) = \mathsf{mod}(b, m)$	Apply Lemma1_2: 1
4.	$(\mathsf{mod}(a, m) = \mathsf{mod}(b, m) \to \mathsf{Congruent}(a, b, m)) \wedge$ $(\mathsf{Congruent}(a, b, m) \to \mathsf{mod}(a, m) = \mathsf{mod}(b, m))$	Intro $\wedge$: 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 $a \equiv_m b$.

Formal: Try it yourself here.

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

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

Formal: Try it yourself here.

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

With those in hand, we prove this as follows.

Formal: Try it yourself here.

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 $d \mid b$.

Formal: Try it yourself here. (Note: you will need `substitute` as well as `algebra`.)

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 $d \mid a \bmod b$.

Formal: Try it yourself here. (Note: you will need `substitute` as well as `algebra`.)

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 $\forall x\,(((x \mid a) \land (x \mid b)) \to ((x \mid c) \land (x \mid d)))$.

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

$$\begin{aligned}
\text{GCD Pos:}\quad & \forall a\,\forall b\,(\top \to (((\gcd(a,b) \mid a) \land (\gcd(a,b) \mid b)) \land \forall d\,(((d \mid a) \land d \mid b)) \to (d \mid \gcd(a,b))))\\
\text{GCD Unique:}\quad & \forall a\,\forall b\,\forall x\,(((x \mid a) \land (x \mid b) \land \forall d\,(((d \mid a) \land (d \mid b)) \to (d \le x))) \to (x = \gcd(a,b)))
\end{aligned}$$

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

Formal: Try it yourself here.

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 $\gcd(a,b) \le \gcd(c,d)$.

Lemma 4

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

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

$$\begin{aligned}
\text{LessOrEqual:}\quad & \forall a\,\forall b\,((a \le b) \to ((a = b) \lor (a < b)))\\
\text{LessVsGreater:}\quad & \forall a\,\forall b\,((a < b) \to \neg(b < a))
\end{aligned}$$

The first fact is the definition of "$\le$". The says that "$<$" is anti-symmetric.

Formal: Try it yourself here. (Hint: Prove it by cases over $a < b$ and $\neg(a < b)$.)

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

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

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