thm_2Earithmetic_2EMOD_MULT_MOD (TMPubrQau1V2wC1S9iGyk7nKk9hrdm9wJ8H)

October 26, 2020

Let $c\_2Enum\_2EZERO\_\_REP : \iota$ be given. Assume the following.

$$c\_2Enum\_2EZERO\_\_REP \in omega \tag{1}$$

Let $ty\_2Enum\_2Enum : \iota$ be given. Assume the following.

$$nonempty\ ty\_2Enum\_2Enum \tag{2}$$

Let $c\_2Enum\_2EABS\_num : \iota$ be given. Assume the following.

$$c\_2Enum\_2EABS\_num \in (ty\_2Enum\_2Enum^{omega}) \tag{3}$$

Definition 1 *We define* c_2Emin_2E_3D *to be* $\lambda A.\lambda x \in A.\lambda y \in A.inj\_\_o\ (x = y)$
of type $\iota \Rightarrow \iota$.

Definition 2 *We define* c_2Enum_2E0 *to be* $(ap\ c\_2Enum\_2EABS\_num\ c\_2Enum\_2EZERO\_\_REP)$.

Definition 3 *We define* c_2Earithmetic_2EZERO *to be* c_2Enum_2E0.

Let $c\_2Enum\_2EREP\_\_num : \iota$ be given. Assume the following.

$$c\_2Enum\_2EREP\_\_num \in (omega^{ty\_2Enum\_2Enum}) \tag{4}$$

Let $c\_2Enum\_2ESUC\_\_REP : \iota$ be given. Assume the following.

$$c\_2Enum\_2ESUC\_\_REP \in (omega^{omega}) \tag{5}$$

Definition 4 *We define* c_2Ebool_2ET *to be* $(ap\ (ap\ (\text{c\_2Emin\_2E\_3D}\ (2^2))\ (\lambda V0x \in 2.V0x))\ (\lambda V1x \in 2.V1$

Definition 5 *We define* c_2Ebool_2E_21 *to be* $\lambda A\_27a : \iota.(\lambda V0P \in (2^{A\_27a}).(ap\ (ap\ (\text{c\_2Emin\_2E\_3D}\ (2^{A\_27})$

Definition 6 *We define* c_2Enum_2ESUC *to be* $\lambda V0m \in ty\_2Enum\_2Enum.(ap\ c\_2Enum\_2EABS\_num\ ($

Let $c\_2Earithmetic\_2E\_2B : \iota$ be given. Assume the following.

$$c\_2Earithmetic\_2E\_2B \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum}) \tag{6}$$

1

Definition 7 *We define* c_2Earithmetic_2EBIT1 *to be* $\lambda V0n \in ty\_2Enum\_2Enum.(ap\ (ap\ c\_2Earithmetic\_$

Definition 8 *We define* c_2Earithmetic_2ENUMERAL *to be* $\lambda V0x \in ty\_2Enum\_2Enum.V0x.$

Definition 9 *We define* c_2Emin_2E_40 *to be* $\lambda A.\lambda P \in 2^A.\textbf{if}\ (\exists x \in A.p\ (ap\ P\ x))\ \textbf{then}\ (the\ (\lambda x.x \in A \wedge p$
of type $\iota \Rightarrow \iota.$

Definition 10 *We define* c_2Ebool_2E_3F *to be* $\lambda A\_27a : \iota.(\lambda V0P \in (2^{A\_27a}).(ap\ V0P\ (ap\ (\text{c\_2Emin\_2E\_40}$

Let $c\_2Earithmetic\_2E\_2A : \iota$ be given. Assume the following.

$$c\_2Earithmetic\_2E\_2A \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum})$$

$$(7)$$

Let $c\_2Earithmetic\_2EMOD : \iota$ be given. Assume the following.

$$c\_2Earithmetic\_2EMOD \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum})$$

$$(8)$$

Definition 11 *We define* c_2Ebool_2EF *to be* $(ap\ (\text{c\_2Ebool\_2E\_21}\ 2)\ (\lambda V0t \in 2.V0t)).$

Definition 12 *We define* c_2Emin_2E_3D_3D_3E *to be* $\lambda P \in 2.\lambda Q \in 2.inj\_o\ (p\ P \Rightarrow p\ Q)$
of type $\iota.$

Definition 13 *We define* c_2Ebool_2E_2F_5C *to be* $(\lambda V0t1 \in 2.(\lambda V1t2 \in 2.(ap\ (\text{c\_2Ebool\_2E\_21}\ 2)\ (\lambda V2t \in$

Definition 14 *We define* c_2Ebool_2E_7E *to be* $(\lambda V0t \in 2.(ap\ (ap\ \text{c\_2Emin\_2E\_3D\_3D\_3E}\ V0t)\ \text{c\_2Ebool\_2E}$

Definition 15 *We define* c_2Eprim__rec_2E_3C *to be* $\lambda V0m \in ty\_2Enum\_2Enum.\lambda V1n \in ty\_2Enum\_2Enu$

Assume the following.

$$(\forall V0m \in ty\_2Enum\_2Enum.(\forall V1n \in ty\_2Enum\_2Enum.($$
$$((ap\ (ap\ c\_2Earithmetic\_2E\_2B\ \text{c\_2Enum\_2E0})\ V0m) = V0m) \wedge (((ap\ ($$
$$ap\ c\_2Earithmetic\_2E\_2B\ V0m)\ \text{c\_2Enum\_2E0}) = V0m) \wedge (((ap\ (ap\ c\_2Earithmetic\_2E\_2B$$
$$(ap\ \text{c\_2Enum\_2ESUC}\ V0m))\ V1n) = (ap\ \text{c\_2Enum\_2ESUC}\ (ap\ (ap\ c\_2Earithmetic\_2E\_2B$$
$$V0m)\ V1n))) \wedge ((ap\ (ap\ c\_2Earithmetic\_2E\_2B\ V0m)\ (ap\ \text{c\_2Enum\_2ESUC}$$
$$V1n)) = (ap\ \text{c\_2Enum\_2ESUC}\ (ap\ (ap\ c\_2Earithmetic\_2E\_2B\ V0m)\ V1n))))))))$$

$$(9)$$

Assume the following.

$$(\forall V0m \in ty\_2Enum\_2Enum.(\forall V1n \in ty\_2Enum\_2Enum.($$
$$((ap\ (ap\ c\_2Earithmetic\_2E\_2A\ \text{c\_2Enum\_2E0})\ V0m) = \text{c\_2Enum\_2E0}) \wedge$$
$$(((ap\ (ap\ c\_2Earithmetic\_2E\_2A\ V0m)\ \text{c\_2Enum\_2E0}) = \text{c\_2Enum\_2E0}) \wedge$$
$$(((ap\ (ap\ c\_2Earithmetic\_2E\_2A\ (ap\ \text{c\_2Earithmetic\_2ENUMERAL}$$
$$(ap\ \text{c\_2Earithmetic\_2EBIT1}\ \text{c\_2Earithmetic\_2EZERO})))\ V0m) = V0m) \wedge$$
$$(((ap\ (ap\ c\_2Earithmetic\_2E\_2A\ V0m)\ (ap\ \text{c\_2Earithmetic\_2ENUMERAL}$$
$$(ap\ \text{c\_2Earithmetic\_2EBIT1}\ \text{c\_2Earithmetic\_2EZERO}))) = V0m) \wedge ($$
$$((ap\ (ap\ c\_2Earithmetic\_2E\_2A\ (ap\ \text{c\_2Enum\_2ESUC}\ V0m))\ V1n) = (ap$$
$$(ap\ c\_2Earithmetic\_2E\_2B\ (ap\ (ap\ c\_2Earithmetic\_2E\_2A\ V0m)\ V1n))$$
$$V1n)) \wedge ((ap\ (ap\ c\_2Earithmetic\_2E\_2A\ V0m)\ (ap\ \text{c\_2Enum\_2ESUC}\ V1n)) =$$
$$(ap\ (ap\ c\_2Earithmetic\_2E\_2B\ V0m)\ (ap\ (ap\ c\_2Earithmetic\_2E\_2A$$
$$V0m)\ V1n)))))))))))$$

$$(10)$$

2

Assume the following.

$$(\forall V0m \in ty\_2Enum\_2Enum.(\forall V1n \in ty\_2Enum\_2Enum.(\\ (ap\ (ap\ c\_2Earithmetic\_2E\_2A\ V0m)\ V1n) = (ap\ (ap\ c\_2Earithmetic\_2E\_2A \\ V1n)\ V0m))))$$

(11)

Assume the following.

$$(\forall V0m \in ty\_2Enum\_2Enum.(\forall V1n \in ty\_2Enum\_2Enum.(\\ \forall V2p \in ty\_2Enum\_2Enum.((ap\ (ap\ c\_2Earithmetic\_2E\_2A\ V0m) \\ (ap\ (ap\ c\_2Earithmetic\_2E\_2A\ V1n)\ V2p)) = (ap\ (ap\ c\_2Earithmetic\_2E\_2A \\ (ap\ (ap\ c\_2Earithmetic\_2E\_2A\ V0m)\ V1n))\ V2p)))))$$

(12)

Assume the following.

$$(\forall V0k \in ty\_2Enum\_2Enum.(\forall V1n \in ty\_2Enum\_2Enum.(\\ (p\ (ap\ (ap\ \mathsf{c\_2Eprim\_\_rec\_2E\_3C}\ \mathsf{c\_2Enum\_2E0})\ V1n)) \Rightarrow (\exists V2r \in \\ ty\_2Enum\_2Enum.(\exists V3q \in ty\_2Enum\_2Enum.((V0k = (ap\ (ap\ c\_2Earithmetic\_2E\_2B \\ (ap\ (ap\ c\_2Earithmetic\_2E\_2A\ V3q)\ V1n))\ V2r)) \wedge (p\ (ap\ (ap\ \mathsf{c\_2Eprim\_\_rec\_2E\_3C} \\ V2r)\ V1n))))))))$$

(13)

Assume the following.

$$(\forall V0n \in ty\_2Enum\_2Enum.(\forall V1r \in ty\_2Enum\_2Enum.(\\ (p\ (ap\ (ap\ \mathsf{c\_2Eprim\_\_rec\_2E\_3C}\ V1r)\ V0n)) \Rightarrow (\forall V2q \in ty\_2Enum\_2Enum. \\ ((ap\ (ap\ c\_2Earithmetic\_2EMOD\ (ap\ (ap\ c\_2Earithmetic\_2E\_2B\ (ap \\ (ap\ c\_2Earithmetic\_2E\_2A\ V2q)\ V0n))\ V1r))\ V0n) = V1r)))))$$

(14)

Assume the following.

$$(\forall V0n \in ty\_2Enum\_2Enum.((p\ (ap\ (ap\ \mathsf{c\_2Eprim\_\_rec\_2E\_3C} \\ \mathsf{c\_2Enum\_2E0})\ V0n)) \Rightarrow (\forall V1q \in ty\_2Enum\_2Enum.(\forall V2r \in \\ ty\_2Enum\_2Enum.((ap\ (ap\ c\_2Earithmetic\_2EMOD\ (ap\ (ap\ c\_2Earithmetic\_2E\_2B \\ (ap\ (ap\ c\_2Earithmetic\_2E\_2A\ V1q)\ V0n))\ V2r))\ V0n) = (ap\ (ap\ c\_2Earithmetic\_2EMOD \\ V2r)\ V0n))))))$$

(15)

Assume the following.
$$True$$

(16)

Assume the following.

$$(\forall V0t1 \in 2.(\forall V1t2 \in 2.(((p\ V0t1) \Rightarrow (p\ V1t2)) \Rightarrow (((p \\ V1t2) \Rightarrow (p\ V0t1)) \Rightarrow ((p\ V0t1) \Leftrightarrow (p\ V1t2)))))$$

(17)

Assume the following.

$$(\forall V0t \in 2.(False \Rightarrow (p\ V0t)))$$

(18)

3

Assume the following.

$$(\forall V0t \in 2.(((True \land (p\ V0t)) \Leftrightarrow (p\ V0t)) \land ((((p\ V0t) \land True) \Leftrightarrow$$
$$(p\ V0t)) \land (((False \land (p\ V0t)) \Leftrightarrow False) \land ((((p\ V0t) \land False) \Leftrightarrow False) \land \qquad (19)$$
$$(((p\ V0t) \land (p\ V0t)) \Leftrightarrow (p\ V0t)))))))$$

Assume the following.

$$(\forall V0t \in 2.(((True \Rightarrow (p\ V0t)) \Leftrightarrow (p\ V0t)) \land ((((p\ V0t) \Rightarrow True) \Leftrightarrow$$
$$True) \land (((False \Rightarrow (p\ V0t)) \Leftrightarrow True) \land ((((p\ V0t) \Rightarrow (p\ V0t)) \Leftrightarrow True) \land ((\qquad (20)$$
$$(p\ V0t) \Rightarrow False) \Leftrightarrow (\neg (p\ V0t))))))))$$

Assume the following.

$$\forall A\_27a.nonempty\ A\_27a \Rightarrow (\forall V0x \in A\_27a.(\forall V1y \in$$
$$A\_27a.((V0x = V1y) \Leftrightarrow (V1y = V0x)))) \qquad (21)$$

Assume the following.

$$(\forall V0t \in 2.(((True \Leftrightarrow (p\ V0t)) \Leftrightarrow (p\ V0t)) \land ((((p\ V0t) \Leftrightarrow True) \Leftrightarrow$$
$$(p\ V0t)) \land (((False \Leftrightarrow (p\ V0t)) \Leftrightarrow (\neg (p\ V0t))) \land (((p\ V0t) \Leftrightarrow False) \Leftrightarrow (\neg (\qquad (22)$$
$$p\ V0t)))))))$$

Assume the following.

$$(\forall V0P \in (2^{ty\_2Enum\_2Enum}).(((p\ (ap\ V0P\ \mathsf{c\_2Enum\_2E0})) \land$$
$$(\forall V1n \in ty\_2Enum\_2Enum.((p\ (ap\ V0P\ V1n)) \Rightarrow (p\ (ap\ V0P\ (ap\ \mathsf{c\_2Enum\_2ESUC}$$
$$V1n)))))) \Rightarrow (\forall V2n \in ty\_2Enum\_2Enum.(p\ (ap\ V0P\ V2n)))))$$
$$(23)$$

Assume the following.

$$(\forall V0n \in ty\_2Enum\_2Enum.(\neg (p\ (ap\ (ap\ \mathsf{c\_2Eprim\_\_rec\_2E\_3C}$$
$$V0n)\ \mathsf{c\_2Enum\_2E0})))) \qquad (24)$$

Assume the following.

$$(\forall V0n \in ty\_2Enum\_2Enum.(p\ (ap\ (ap\ \mathsf{c\_2Eprim\_\_rec\_2E\_3C}\ \mathsf{c\_2Enum\_2E0})$$
$$(ap\ \mathsf{c\_2Enum\_2ESUC}\ V0n))))$$
$$(25)$$

Theorem 1

$$(\forall V0m \in ty\_2Enum\_2Enum.(\forall V1n \in ty\_2Enum\_2Enum.($$
$$((p\ (ap\ (ap\ \mathsf{c\_2Eprim\_\_rec\_2E\_3C}\ \mathsf{c\_2Enum\_2E0})\ V1n)) \land (p\ (ap\ (ap\ \mathsf{c\_2Eprim\_\_rec\_2E\_3C}$$
$$\mathsf{c\_2Enum\_2E0})\ V0m))) \Rightarrow (\forall V2x \in ty\_2Enum\_2Enum.((ap\ (ap\ c\_2Earithmetic\_2EMOD$$
$$(ap\ (ap\ c\_2Earithmetic\_2EMOD\ V2x)\ (ap\ (ap\ c\_2Earithmetic\_2E\_2A$$
$$V1n)\ V0m)))\ V1n) = (ap\ (ap\ c\_2Earithmetic\_2EMOD\ V2x)\ V1n))))))$$

4