thm_2Egcd_2EGCD__IS__GREATEST__COMMON__DIVISOR (TMHY9QhRVJtAdrvr6AufHWXum5PaBdHAkm8)

October 26, 2020

Definition 1 *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* ι.

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

$$nonempty\ ty\_2Enum\_2Enum \tag{1}$$

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

$$c\_2Earithmetic\_2E\_2A \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum}) \tag{2}$$

Definition 2 *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 3 *We define* c_2Emin_2E_40 *to be* $\lambda A.\lambda P \in 2^A$.**if** $(\exists x \in A.p\ (ap\ P\ x))$ **then** $(the\ (\lambda x.x \in A \wedge p$ *of type* $\iota \Rightarrow \iota$.

Definition 4 *We define* c_2Ebool_2E_3F *to be* $\lambda A\_27a : \iota.(\lambda V0P \in (2^{A\_27a}).(ap\ V0P\ (ap$ (c_2Emin_2E_40 A

Definition 5 *We define* c_2Ebool_2ET *to be* $(ap\ (ap$ (c_2Emin_2E_3D $(2^2))\ (\lambda V0x \in 2.V0x))\ (\lambda V1x \in 2.V1$

Definition 6 *We define* c_2Ebool_2E_21 *to be* $\lambda A\_27a : \iota.(\lambda V0P \in (2^{A\_27a}).(ap\ (ap$ (c_2Emin_2E_3D $(2^{A\_27}$

Definition 7 *We define* c_2Edivides_2Edivides *to be* $\lambda V0a \in ty\_2Enum\_2Enum.\lambda V1b \in ty\_2Enum\_2Enum$

Definition 8 *We define* c_2Ebool_2E_2F_5C *to be* $(\lambda V0t1 \in 2.(\lambda V1t2 \in 2.(ap$ (c_2Ebool_2E_21 2) $(\lambda V2t \in 2$

Let $c\_2Egcd\_2Egcd : \iota$ be given. Assume the following.

$$c\_2Egcd\_2Egcd \in ((ty\_2Enum\_2Enum^{ty\_2Enum\_2Enum})^{ty\_2Enum\_2Enum}) \tag{3}$$

Definition 9 *We define* c_2Egcd_2Eis__gcd *to be* $\lambda V0a \in ty\_2Enum\_2Enum.\lambda V1b \in ty\_2Enum\_2Enum.\lambda V$

Assume the following.

$$(\forall V0a \in ty\_2Enum\_2Enum.(\forall V1b \in ty\_2Enum\_2Enum.(p\ (ap\ (ap\ (ap\ \mathsf{c\_2Egcd\_2Eis\_\_gcd}\ V0a)\ V1b)\ (ap\ (ap\ c\_2Egcd\_2Egcd\ V0a) V1b)))))) \tag{4}$$

Theorem 1

$$(\forall V0a \in ty\_2Enum\_2Enum.(\forall V1b \in ty\_2Enum\_2Enum.((p\ (ap\ (ap\ \mathsf{c\_2Edivides\_2Edivides}\ (ap\ (ap\ c\_2Egcd\_2Egcd\ V0a)\ V1b)) V0a))\wedge((p\ (ap\ (ap\ \mathsf{c\_2Edivides\_2Edivides}\ (ap\ (ap\ c\_2Egcd\_2Egcd V0a)\ V1b))\ V1b))\wedge(\forall V2d \in ty\_2Enum\_2Enum.(((p\ (ap\ (ap\ \mathsf{c\_2Edivides\_2Edivides} V2d)\ V0a))\wedge(p\ (ap\ (ap\ \mathsf{c\_2Edivides\_2Edivides}\ V2d)\ V1b)))\Rightarrow(p\ (ap (ap\ \mathsf{c\_2Edivides\_2Edivides}\ V2d)\ (ap\ (ap\ c\_2Egcd\_2Egcd\ V0a)\ V1b)))))))))$$