Chapter 8
Arithmetic in Peano Arithmetic

In this chapter we take a closer look at Peano Arithmetic (PA) which we have defined in Chapter 1. In particular, we prove within PA some basic arithmetial results starting with the commutativity and associativity of addition and multiplication, culminating in some results about coprimality. This paves the way for the coding of finite sequences of numbers which will be covered in the next chapter. Furthermore, we introduce some alternative formulations of the induction principle PA_6.

Addition & Multiplication

In this section we verify the basic computation rules involving addition and multiplication. Since the complete proofs are very long and tedious, we will show only commutativity of "+" in a elaborate way. Subsequently, we will use semi-formal proofs as described in Chapter 1 which include enough details to allow the reader to reconstruct a corresponding formal proof.

LEMMA 8.1. $\mathsf{PA} \vdash \forall x \forall y (x + y = y + x)$

Proof. We proceed by induction on x. Thus, we have to show

(a) $\mathsf{PA} \vdash \forall y (\mathsf{0} + y = y + \mathsf{0})$, and

(b) $\mathsf{PA} \vdash \forall y (x + y = y + x) \to \forall y (\mathsf{s}x + y = y + \mathsf{s}x)$.

For (a), we first prove

$$\vdash_{\mathsf{PA}} \forall y (\mathsf{0} + y = y)$$

by induction on y. The base case $\mathsf{0} + \mathsf{0} = \mathsf{0}$ is clearly an instance of PA_2 and for the induction step assume $\mathsf{0} + y = y$ for some y. Then $\mathsf{0} + \mathsf{s}y = \mathsf{s}(\mathsf{0} + y)$ by PA_3 and $\mathsf{s}(\mathsf{0} + y) = \mathsf{s}y$ by assumption. To keep the notation short we just write $\mathsf{0} + \mathsf{s}y = \mathsf{s}(\mathsf{0} + y) = \mathsf{s}y$ instead of $\mathsf{0} + \mathsf{s}y = \mathsf{s}(\mathsf{0} + y) \wedge \mathsf{s}(\mathsf{0} + y) = \mathsf{s}y$. So, by PA_6

we obtain $\forall y(0 + y = y)$ and since by PA_2 we have $\forall y(y + 0 = y)$, by symmetry and transitivity of "=" we have $\forall y(0 + y = y + 0)$.

As a prerequisite for (b) we need

$$\vdash_{\mathsf{PA}} \forall y(\mathsf{s}x + y = \mathsf{s}(x + y))$$

which again will be verified by induction on y: If $y = 0$, note that by PA_2 we have $\mathsf{s}x + 0 = \mathsf{s}x = \mathsf{s}(x + 0)$. For the induction step assume $\mathsf{s}x + y = \mathsf{s}(x + y)$. Then, by PA_3, we have $\mathsf{s}x + \mathsf{s}y = \mathsf{s}(\mathsf{s}x + y) = \mathsf{s}(\mathsf{s}(x + y)) = \mathsf{s}(x + \mathsf{s}y)$.

Now, we are ready to prove (b): Assume that $x + y = y + x$ for some x and for all y. Then $\mathsf{s}x + y = \mathsf{s}(x + y) = \mathsf{s}(y + x) = y + \mathsf{s}x$ by our computation above and PA_3, which, by PA_6, shows (b). ⊣

In a similar manner we can derive other basic calculation rules whose proofs are left as an exercise for the reader.

LEMMA 8.2.

(a) $\mathsf{PA} \vdash \forall x \forall y \forall z((x + y) + z = x + (y + z))$
(b) $\mathsf{PA} \vdash \forall x \forall y \forall z((x \cdot y) \cdot z = x \cdot (y \cdot z))$
(c) $\mathsf{PA} \vdash \forall x \forall y(x \cdot y = y \cdot x)$
(d) $\mathsf{PA} \vdash \forall x \forall y \forall z(x \cdot (y + z) = (x \cdot y) + (x \cdot z))$

From now on, we will make use of these rules without explicitly mentioning them anymore. The next lemma shows injectivity of left — and by commutativity also right — addition.

LEMMA 8.3. $\mathsf{PA} \vdash \forall x \forall y \forall z(x + y = x + z \to y = z)$

Proof. The proof is by induction on x. The base case follows from the proof of LEMMA 8.1. For the induction step assume

$$\forall y \forall z(x + y = x + z \to y = z)$$

and let $\mathsf{s}x + y = \mathsf{s}x + z$. Then $\mathsf{s}(x + y) = \mathsf{s}x + y = \mathsf{s}x + z = \mathsf{s}(x + z)$, where the first and the third equality again follow from LEMMA 8.1 and PA_3. Then by PA_2 we obtain $x + y = x + z$ and in particular $y = z$. ⊣

The next result is crucial, because — as we will see in Chapter 10 — it is the only application of PA_6 which is indispensable for the proof of the FIRST INCOMPLETENESS THEOREM 10.6.

LEMMA 8.4. $\mathsf{PA} \vdash \forall x\big(x = 0 \vee \exists y(x = \mathsf{s}y)\big)$

Proof. We proceed by induction on x. The base case is trivial and the induction step follows from the fact that x witnesses $\exists y(\mathsf{s}x = \mathsf{s}y)$ ⊣

From now on, we will use the convention that "$\cdot$" binds stronger than "$+$" and omit the multplication sign, *e.g.*, the term $xy + z$ stands for $(x \cdot y) + z$. Furthermore, by associativity of "$+$" and "$\cdot$" we may omit brackets when we have pure products of pure sums of terms.

To keep the notatio short, for $\mathscr{L}_{\mathsf{PA}}$-formulae φ we define

$$\forall x \neq 0\, \varphi(x) :\Longleftrightarrow \forall x\big(x \neq 0 \to \varphi(x)\big)\,.$$

The next result shows a property of multiplication, which is similar to the one given in LEMMA 8.3 for addition.

LEMMA 8.5.

(a) $\mathsf{PA} \vdash \forall x \forall y\big(xy = 0 \leftrightarrow (x = 0 \vee y = 0)\big)$

(b) $\mathsf{PA} \vdash \forall x \neq 0\, \forall y \forall z(xy = xz \to y = z)$

Proof. For (a) let $xy = 0$ and suppose towards a contradiction that $x, y \neq 0$. Then by LEMMA 8.4 there are x', y' such that $x = \mathsf{s}x'$ and $y = \mathsf{s}y'$. By PA_5 and PA_3, we obtain

$$0 = xy = \mathsf{s}x' \cdot \mathsf{s}y' = \mathsf{s}x' \cdot y' + \mathsf{s}x' = \mathsf{s}(\mathsf{s}x' \cdot y' + x')\,,$$

which contradicts PA_0.

For (b) suppose that $x \neq 0$. We proceed by induction on y. If $y = 0$, then $xy = 0$. So, $xy = xz$ implies $xz = 0$ and by (a) we obtain $z = 0$ and consequently $y = z$. Now assume that

$$\forall z(xy = xz \to y = z).$$

Let z be arbitrary such that $x \cdot \mathsf{s}y = xz$. By refinj, we can rule out the possibility that $z = 0$, hence, by LEMMA 8.4, there is a z' such that $z = \mathsf{s}z'$. Therefore, by PA_5,

$$xy + x = x \cdot \mathsf{s}y = xz = x \cdot \mathsf{s}z' = xz' + x\,.$$

Using LEMMATA 8.1 and 8.3 we obtain that $xy = xz'$ and thus the induction hypothesis implies $y = z'$. So, we finally get $\mathsf{s}y = \mathsf{s}z' = z$ as desired. ⊣

The Natural Ordering on Natural Numbers

In Chapter 6 we have seen how to extend languages by incorporating new symbols for relations, functions or constants. In this sense we can now introduce the binary relations $\leq$ and $<$ in PA by stipulating

$$x \leq y :\Longleftrightarrow \exists r(x + r = y)\,,$$

$$x < y :\Longleftrightarrow x \leq y \wedge x \neq y\,.$$

An alternative definition of $x < y$ is given by

$$x < y :\Longleftrightarrow \exists r \neq 0\,(x + r = y)\,.$$

Furthermore, we define

$$x \geq y :\Longleftrightarrow y \leq x$$
$$x > y :\Longleftrightarrow y < x.$$

Now, we define **bounded quantification** by stipulating:

$$\exists x \lhd y\, \varphi(x) :\Longleftrightarrow \exists x\big(x \lhd y \wedge \varphi(x)\big),$$

$$\forall x \lhd y\, \varphi(x) :\Longleftrightarrow \forall x\big(x \lhd y \to \varphi(x)\big),$$

where "$\lhd$" stands either for "$<$" or for "$\leq$". The next result shows some properties of "$<$" and "$\leq$".

LEMMA 8.6.

(a) $\mathsf{PA} \vdash \forall x \forall y (x < \mathtt{s}y \leftrightarrow x \leq y)$

(b) $\mathsf{PA} \vdash \forall x \forall y (x < y \leftrightarrow \mathtt{s}x \leq y)$

Proof. We only consider (a) and leave (b) as an excercise. Fix x and y. Firstly, assume that $x < \mathtt{s}y$ and take $r \neq 0$ such that $x + r = \mathtt{s}y$. By LEMMA 8.4 we find an r' such that $r = \mathtt{s}r'$. Then $\mathtt{s}(x + r') = x + \mathtt{s}r' = x + r = \mathtt{s}y$ by PA_3, and by PA_2 we obtain $x + r' = y$ which shows that $x \leq y$.

Conversely, let $x \leq y$ and take r such that $x+r = y$. Then $x+\mathtt{s}r = \mathtt{s}(x+r) = \mathtt{s}y$ which shows that $x < \mathtt{s}y$. ⊣

The next result implies that "$\leq$" defines a total ordering on the natural numbers.

LEMMA 8.7.

(a) $\mathsf{PA} \vdash \forall x (x \leq x)$

(b) $\mathsf{PA} \vdash \forall x \forall y (x \leq y \wedge y \leq x \to x = y)$

(c) $\mathsf{PA} \vdash \forall x \forall y \forall z (x \leq y \wedge y \leq z \to x \leq z)$

(d) $\mathsf{PA} \vdash \forall x \forall y (x < y \vee x = y \vee x > y)$

Proof. Condition (a) is a trivial consequence of PA_2.

For (b) assume that $x \leq y$ and $y \leq x$. Then there are r, s such that $x + r = y$ and $y + s = x$. We obtain that

$$y + (s + r) = (y + s) + r = x + r = y = y + 0,$$

and by LEMMA 8.3, this implies $s + r = 0$ and hence, by PA_0, $s = 0 = r$, which shows that $x = y$.

For (c) let $x \leq y$ and $y \leq z$ and take witnesses r, s satisfying $x + r = y$ and $y + s = z$. Then $x + (r + s) = (x + r) + s = y + s = z$ and thus $x \leq z$.

We show (d) by induction on x. If $x = \mathtt{0}$, we can make a case distinction according to LEMMA 8.4: If $y = \mathtt{0}$ then $x = y$ and otherwise $x < y$. For the induction step fix y and assume that $x < y \vee x = y \vee x > y$. Now, we make a case distinction, where in the case that $x < y$, LEMMA 8.6 implies that $\mathtt{s}x \leq y$ and thus either $\mathtt{s}x < y$ or $\mathtt{s}x = y$. Secondly, if $x = y$ then

$$\mathtt{s}x = \mathtt{s}y = \mathtt{s}(y + \mathtt{0}) = y + \mathtt{s0}$$

which shows that $\mathtt{s}x > y$. The case when $x > y$ is similar. ⊣

Finally, one can show that addition and multiplication with non-zero numbers preserve the natural odering (the proof is left as an excercise to the reader):

LEMMA 8.8.

(a) $\mathsf{PA} \vdash \forall x \forall y \forall z \big(x \leq y \leftrightarrow (x + z \leq y + z)\big)$

(b) $\mathsf{PA} \vdash \forall x \forall y \forall z \neq \mathtt{0} \big(x \leq y \leftrightarrow (x \cdot z \leq y \cdot z)\big)$

Subtraction & Divisibility

With the help of the ordering that we have introduced in the previous section, we are ready to define a version of subtraction which rounds up to $\mathtt{0}$ in order to preserve non-negativity. For this, we first show the following

LEMMA 8.9. $\mathsf{PA} \vdash \forall x \forall y \big(x \leq y \to \exists! r (x + r = y)\big)$

Proof. Assume that $x \leq y$. The existence of r follows directly from the definition of "$\leq$" and the uniqueness of r is a consequence of LEMMA 8.3. ⊣

So, we can define within PA the binary function "$-$", called **bounded subtraction**, by stipulating

$$x - y = z :\Longleftrightarrow (y \leq x \wedge y + z = x) \vee (x < y \wedge z = \mathtt{0})\,.$$

Observe that $\mathsf{PA} \vdash \forall x \forall y \leq x((x - y) + y = x)$, from which we can easily derive computation rules for bounded subtraction such as

$$\mathsf{PA} \vdash \forall x \forall y \forall z \big(x(y - z) = xy - xz\big), \quad \text{or}$$

$$\mathsf{PA} \vdash \forall x \forall y \forall z \big(x \leq y \to (x - z \leq y - z)\big).$$

Let us turn now to divisibility, which can easily be formalised by stipulating

$$x \,|\, y :\Longleftrightarrow \exists r (rx = y).$$

If the binary divisibility relation "$\mid$" holds for the ordered pair (x, y), then we say that "x *divides* y". Without much effort, one can verify that the divisibility relation is reflexive, antisymmetric, and transitive. So, we will omit the proof of the next result.

LEMMA 8.10.

(a) $\mathsf{PA} \vdash \forall x(x \mid x)$

(b) $\mathsf{PA} \vdash \forall x \forall y(x \mid y \wedge y \mid x \to x = y)$

(c) $\mathsf{PA} \vdash \forall x \forall y \forall z(x \mid y \wedge y \mid z \to x \mid z)$

Also without much effort we can prove the following

LEMMA 8.11.

(a) $\mathsf{PA} \vdash \forall x \forall y \forall z(x \mid y \wedge x \mid z \to x \mid y \pm z)$, *where the symbol "*$\pm$*" stands for either "*$+$*" or "*$-$*".*

(b) $\mathsf{PA} \vdash \forall x \forall y \forall z(x \mid y \to x \mid yz)$

Proof. For (a) assume that x divides y and z. Then there are r, s such that $y = rx$ and $z = sx$. Then $y \pm z = rx \pm sx = (r \pm s)x$, thus x divides $y \pm z$. Condition (b) is obvious. ⊣

In most textbooks, one defines two numbers to be *coprime* (or *relatively prime*), if they have no common divisor. Nevertheless, for our purpose it is more convenient to use the following equivalent definition:

$$\mathrm{coprime}(x, y) \;:\Longleftrightarrow\; x \neq 0 \wedge y \neq 0 \wedge \forall z\big(x \mid yz \to x \mid z\big)$$

Since we are working with this somewhat unusual definition of relative primality, we first check that it is a symmetric relation.

LEMMA 8.12. $\mathsf{PA} \vdash \forall x \forall y\big(\mathrm{coprime}(x, y) \leftrightarrow \mathrm{coprime}(y, x)\big)$

Proof. Assume $\mathrm{coprime}(x, y)$. We have to show that for every z we have $y \mid xz$ implies $y \mid z$. So, let z be such that $y \mid xz$. Since $y \mid xz$, there is an r with $yr = xz$. Furthermore, since $x \mid xz$ and $xz = yr$, we get $x \mid yr$, and by $\mathrm{coprime}(x, y)$ we have $x \mid r$. Thus, there is an s such that $xs = r$, and hence, $xsy = ry = yr = xz$. Now, by LEMMA 8.5 we obtain $sy = z$, and therefore $y \mid z$, as desired. ⊣

If the binary relation "coprime" holds for x and y, then we say that "x *and* y are *coprime*".

LEMMA 8.13. $\mathsf{PA} \vdash \forall x \forall y \forall k\big(k \mid x \wedge \mathrm{coprime}(x, y) \to \mathrm{coprime}(k, y)\big)$.

Proof. Assume that x and y are coprime. Let k be a divisor of x and let r be such that $rk = x$. Assume $y \mid kz$ for some arbitrary z. We have to show that $y \mid z$. First notice that by LEMMA 8.11 (b), $y \mid rkz$, and since $rkz = xz$, we have $y \mid xz$. Now, since $\mathrm{coprime}(x, y)$, we obtain $y \mid z$ as desired. ⊣

The following result will be crucial in the construction of *Gödel's β-function* (see THEOREM 9.8), which will be the key to the FIRST INCOMPLETENESS THEOREM 10.6.

LEMMA 8.14. $\mathsf{PA} \vdash \forall k \forall x \neq \mathsf{0}\, \forall j \Big(k \mid x \to \mathrm{coprime}\big(\mathsf{1} + (j+k)x, \mathsf{1} + jx\big)\Big)$

Proof. We first show $\mathsf{PA} \vdash \forall x \neq \mathsf{0}\, \forall j \big(\mathrm{coprime}(x, \mathsf{1} + jx)\big)$, *i.e.*, we show that for all z,

$$x \mid (\mathsf{1} + jx)z \;\to\; x \mid z\,.$$

For this, suppose $x \mid (\mathsf{1} + jx)z$ for some arbitrary z. Since $(\mathsf{1} + jx)z = z + jxz$, by LEMMA 8.11 (b) we have $x \mid jxz$, and as a consequence of LEMMA 8.11 (a) we obtain $x \mid z$.

Now, let k and $x \neq \mathsf{0}$ be such that $k \mid x$. Notice that since $x \neq \mathsf{0}$, this implies that $k \neq \mathsf{0}$. Furthermore, let j be arbitrary but fixed. We have to show

$$\mathrm{coprime}\big(\mathsf{1} + jx, \mathsf{1} + (j+k)x\big)\,,$$

i.e., we have to show that for all z,

$$(\mathsf{1} + jx) \mid \big(\mathsf{1} + (j+k)x\big)z \;\to\; (\mathsf{1} + jx) \mid z\,.$$

First notice that

$$\big(\mathsf{1} + (j+k)x\big)z = (\mathsf{1} + jx + kx)z = (\mathsf{1} + jx)z + kxz\,.$$

Assume now that for some z,

$$(\mathsf{1} + jx) \mid (\mathsf{1} + jx)z + kxz\,.$$

By LEMMA 8.11 (b) we have $(\mathsf{1} + jx) \mid (\mathsf{1} + jx)z$, and by LEMMA 8.11 (a), this implies $(\mathsf{1} + jx) \mid kxz$. Now, since $\mathrm{coprime}(x, \mathsf{1} + jx)$, as shown above, we get

$$(\mathsf{1} + jx) \mid x(kz) \to (\mathsf{1} + jx) \mid kz\,.$$

Finally, since by assumption $k \mid x$, by LEMMA 8.13 and $\mathrm{coprime}(x, \mathsf{1} + jx)$ we get $\mathrm{coprime}(k, \mathsf{1} + jx)$. Hence, we obtain $(\mathsf{1} + jx) \mid z$ as desired. ⊣

Alternative Induction Schemata

A fundamental principle in elementary number theory states that if there is a natural number fulfilling some property Ψ, then there must be a least natural number satisfying Ψ. This principle can be shown in PA; actually, every instance of this principle (*i.e.*, by considering Ψ to be some $\mathscr{L}_{\mathsf{PA}}$-formula) is equivalent to the corresponding instance of the induction schema PA_6. In order to prove this, we need another induction principle which will also turn out to be quite useful.

PROPOSITION 8.15 (STRONG INDUCTION PRINCIPLE). *Let $\varphi(x)$ be an $\mathscr{L}_{\mathsf{PA}}$-formula. Then in* PA, *$\varphi$ satisfies the following* ***principle of strong induction****:*

$$\mathsf{PA} \vdash \forall x\big(\forall y < x\, \varphi(y) \to \varphi(x)\big) \to \forall x \varphi(x)$$

Proof. Suppose $\forall x\big(\forall y < x\, \varphi(y) \to \varphi(x)\big)$. Using PA_6, we first show $\forall x \psi(x)$ for

$$\psi :\equiv \forall y < x\, \varphi(y).$$

Notice that $\psi(\mathsf{0})$ vacuously holds, since there is no $y < \mathsf{0}$ with $\neg\varphi(y)$. Now, if $\psi(x)$ holds, then by our assumption we have $\varphi(x)$. So, we have $\psi(x)$ and $\varphi(x)$, which is the same as $\psi(\mathsf{s}x)$. So, by PA_6 we obtain $\forall x \psi(x)$. Now, because for every x, $\psi(\mathsf{s}x)$ implies $\varphi(x)$, we finally obtain $\forall x \varphi(x)$. ⊣

PROPOSITION 8.16 (LEAST NUMBER PRINCIPLE). *Let $\varphi(x)$ be an $\mathscr{L}_{\mathsf{PA}}$-formula. Then*

$$\mathsf{PA} \vdash \exists x \varphi(x) \to \exists x\big(\varphi(x) \wedge \forall y < x\, \neg\varphi(y)\big).$$

Informally, the LEAST NUMBER PRINCIPLE states that if there is a witness to an arithmetic statement, then there is always a least witness. Often, this is used in the following equivalent form: If a universally quantified formula does not hold, then there is a least counterexample.

Proof of Proposition 8.16. By TAUTOLOGY (K) and the 3-SYMBOLS THEOREM 1.2, we have

$$\exists x \varphi(x) \to \exists x\big(\varphi(x) \wedge \forall y < x\, \neg\varphi(y)\big) \;\Leftrightarrow\; \forall x\, \neg\varphi(x) \vee \exists x\big(\varphi(x) \wedge \forall y < x\, \neg\varphi(y)\big),$$

where the latter is equivalent to the implication

$$\forall x\big(\neg\varphi(x) \vee \neg\forall y < x\, \neg\varphi(y)\big) \to \forall x\, \neg\varphi(x).$$

Now, by TAUTOLOGY (K), this implication is equivalent to

$$\forall x\big(\forall y < x\, \neg\varphi(y) \to \neg\varphi(x)\big) \to \forall x\, \neg\varphi(x),$$

which is the STRONG INDUCTION PRINCIPLE 8.15 applied to the formula $\neg\varphi(x)$, and consequently we have $\mathsf{PA} \vdash \exists x\varphi(x) \to \exists x\big(\varphi(x) \wedge \forall y < x\, \neg\varphi(y)\big)$. ⊣

Relative Primality revisited

We conclude this chapter by providing an alternative definition of relative primality, which shall be useful in the next chapter. First, we introduce the *Principle of Division with Remainder*:

PROPOSITION 8.17 (PRINCIPLE OF DIVISION WITH REMAINDER).

$$\mathsf{PA} \vdash \forall x\, \forall y > \mathsf{0}\, \exists q\, \exists r\big(x = qy + r \wedge r < b\big).$$

Proof. Let $\varphi(x) \equiv \forall y > \mathsf{0}\, \exists q\, \exists r\big(x = qy + r \wedge r < q\big)$. The proof is by induction on x. We obviously have $\varphi(\mathsf{0})$. Now, assume that we have $\varphi(x)$ for some x, *i.e.*, for each $y > \mathsf{0}$ there are q, r such that

$$x = qy + r \wedge r < q\,.$$

If we replace x with $\mathsf{s}x$, then for each $y > \mathsf{0}$ there are q, r such that

$$\mathsf{s}x = qy + \mathsf{s}r \wedge \mathsf{s}r \leq q\,.$$

If $\mathsf{s}r < q$, let $r' := \mathsf{s}r$ and $q' := q$, and if $\mathsf{s}r = q$, let $r' := \mathsf{0}$ and $q' := \mathsf{s}q$. Now, in both cases we obtain

$$\mathsf{s}x = q'y + r' \wedge r' =< q'\,,$$

which shows $\varphi(\mathsf{s}x)$. ⊣

The following result gives a relation between PRINCIPLE OF DIVISION WITH REMAINDER and relatively prime numbers:

LEMMA 8.18. *For any $x, y > \mathsf{0}$ with $x = qy + r$ and $r < q$ we have*

$$\mathsf{PA} \vdash \mathrm{coprime}(y, x) \leftrightarrow \mathrm{coprime}(y, r)\,.$$

Proof. By definition we have $\mathrm{coprime}(y, x) \leftrightarrow \forall z(y \mid xz \to y \mid z)$, and since $x = qy + r$, we obtain

$$\mathrm{coprime}(y, x) \leftrightarrow \forall z(y \mid yqz + rz \to y \mid z)\,.$$

Now, by LEMMA 8.11 we have $(y \mid yqz + rz) \leftrightarrow (y \mid rz)$, and therefore we obtain

$$\mathrm{coprime}(y, x) \;\leftrightarrow\; \forall z(y \mid rz \to y \mid z) \;\leftrightarrow\; \mathrm{coprime}(y, r)\,.$$

⊣

Now we are ready to give the promised alternative definition of relative primality.

PROPOSITION 8.19.

$$\mathsf{PA} \vdash \forall x \forall y \Big(\mathrm{coprime}(x,y) \;\leftrightarrow\; x \neq \mathtt{0} \wedge y \neq \mathtt{0} \wedge \forall z \big((z \mid x \wedge z \mid y) \rightarrow z = \mathtt{1} \big) \Big).$$

Proof. The statement is obvious for $x = y$, or if at least one of x and y is equal to $\mathtt{1}$. So, without loss of generality, let us assume that $x > y > \mathtt{1}$.

($\rightarrow$) The proof is by contraposition. Assume that there is a z such that $z \mid x$, $z \mid y$, and $z > \mathtt{1}$. So, there is a $u < x$ such that $uz = x$. Now, since $z \mid y$, we obtain $x \mid yu$, and since $u < x$, we have $x \nmid u$, which implies $\neg\, \mathrm{coprime}(x,y)$.

($\leftarrow$) Assume towards a contradiction that there is a pair of numbers (x,y) with $x > y > \mathtt{0}$, such that for all z we have

$$(z \mid x \wedge z \mid y) \rightarrow z = \mathtt{1}\,,$$

but $\neg\, \mathrm{coprime}(x,y)$. By the LEAST NUMBER PRINCIPLE, let (x_0, y_0) be the such a pair of numbers where x_0 is minimal. Let q and r be such $x_0 = qy_0 + r$. Since $\neg\, \mathrm{coprime}(x_0, y_0)$, by LEMMA 8.18 we have $\neg\, \mathrm{coprime}(y_0, r)$. On the other hand, if there is a $z_0 > \mathtt{1}$ with $z_0 \mid y_0$ and $z_0 \mid r$, then this would imply that

$$z_0 \mid qy_0 + r\,, \quad \textit{i.e.,}\; z_0 \mid x_0\,,$$

but since $z_0 > \mathtt{1}$, this contradicts the fact that $(z_0 \mid x_0 \wedge z_0 \mid y_0) \rightarrow z_0 = \mathtt{1}$. So, for the pair (y_0, r) we have $\neg\, \mathrm{coprime}(y_0, r)$, for all z we have

$$(z \mid y_0 \wedge z \mid r) \rightarrow z = \mathtt{1}\,,$$

and in addition we have $y_0 < x_0$, which is a contradiction to the minimality of x_0. $\dashv$

As an immediate consequence of PROPOSITION 8.19 we get the following

COROLLARY 8.20. *For all x and y, the following statement is provable in* PA.

$$\mathrm{coprime}(x,y) \;\leftrightarrow\; x \neq \mathtt{0} \wedge y \neq \mathtt{0} \wedge \forall z < (x+y) \big((z \mid x \wedge z \mid y) \rightarrow z = \mathtt{1} \big)$$

EXERCISES

8.0 Prove that addition is associtative, *i.e.*, $\mathsf{PA} \vdash \forall x \forall y \forall z (x + (y + z) = (x + y) + z)$.

8.1 Introduce the unary relations $\mathrm{even}(x)$ and $\mathrm{odd}(x)$ formalising evenness and oddness, and show that

$$\mathsf{PA} \vdash \forall x \big(\mathrm{even}(x) \vee \mathrm{odd}(x) \big).$$

8.2 Show that BÉZOUT'S LEMMA is provable in PA, *i.e.*, show that

$$\mathsf{PA} \vdash \forall x \forall y \Big(\mathrm{coprime}(x, y) \leftrightarrow \big(x \neq \mathsf{0} \wedge y \neq \mathsf{0} \wedge \exists a < y \, \exists b < x \, (ax + \mathsf{1} = by) \big) \Big).$$

Hint: Show first $\exists a \exists b (ax + \mathsf{1} = by) \leftrightarrow \exists a' \exists b' (a'x = b'y + \mathsf{1})$ (*e.g.*, let $a' := y - a$ and $b' := x - b$). Then use the PRINCIPLE OF DIVISION WITH REMAINDER and the LEAST NUMBER PRINCIPLE.

8.3 Prove PA_6 from PA_0–PA_5 and the LEAST NUMBER PRINCIPLE.

8.4 Prove the following alternative induction principle:

$$\mathsf{PA} \vdash \big(\varphi(\mathsf{1}) \wedge \forall x (\varphi(x) \to \varphi(\mathsf{2}x) \wedge \varphi(x - \mathsf{1})) \big) \to \forall x \varphi(x)$$