Answers/Assnmt6/MATH 318/Fall, 2007

[1] PA $\vdash$ $\forall x..x=0 \vee \exists y.x=y+1$

Induction (on x):

Basis: $x=0$. P(0) : $0=0 \vee$ ... : TRUE

Induction step:

Induction hypothesis: $x=0 \vee \exists y.x=y+1$

to show: $Sx=0 \vee \exists y.Sx=y+1$ (1)?

Theorem of PA: $x+1=Sx$ ($L4$) .

Therefore, (1) holds "with $y=x$ ". □

Formal: Abbreviate: $P(x) :=: x=0 \vee \exists y.x=y+1$.

		1	$0=0$	E
P(0)		2	$0=0 \vee \exists y.0=y+1$	T:1
	3	3	$P(x)$	P
		4	$Sx=x+1$	Theorem (of PA)
		5	$\exists y.Sx=y+1$	EG:4
P(Sx)		6	$Sx=0 \vee \exists y.Sx=y+1$	T:5
		7	$P(x)\longrightarrow P(Sx)$	T:6
Ind.Step		8	$\forall x.P(x)\longrightarrow P(Sx)$	UG:7
		9	$P(0) \wedge \forall x.P(x)\longrightarrow P(Sx)$.	T:2,8
		10	$[P(0) \wedge \forall x.P(x)\longrightarrow P(Sx).]\longrightarrow \forall xP(x)$	Thm (MI;AxSc5)
		11	$\forall xP(x)$	T:2,8,11

[2] $\forall x\forall y\forall u.(x+u=y+u\longrightarrow x=y)$

Induction on u : induction statement: $P(u) :=: x+u=y+u\longrightarrow x=y$ ("fixed" x,y)

Basis: $u=0$: $\underbrace{x+0}_{x}=\underbrace{y+0}_{y}\xrightarrow{?} x=y$. □.

Ax1$\rightarrow$

Induction step:

Ind. hyp.: $x+u=y+u\longrightarrow x=y$

to show $x+Su=y+Su\longrightarrow x=y$?

assume $x+Su=y+Su$. By Ax2 , we get $S(x+u)=S(y\| u)$. By Ax 7, we get $x+u=y+u$. By ind. hyp., we get $x=y$ □ .

Formal: Abbreviate: $P(u) :=: x+u=y+u\longrightarrow x=y$.

		1	$[P(0) \wedge \forall u(P(u)\longrightarrow P(Su))]\longrightarrow \forall uP(u)$	
		2	$\forall x.x+0=x$	Thm (Ax1)
		3	$x+0=x$	US:2
		4	$y+0=y$	Us:2
		5	$x=y\longrightarrow x=y$	T
P(0)		6	$x+0=y+0\longrightarrow x=y$	E ($\times$2): 3,4,5
Ind.Hyp: P(u) :				
	7	7	$x+u=y+u\longrightarrow x=y$	P
	8	8	$x+Su=y+Su$	P

	9	$\forall x\forall y(x+Sy = S(x+y)$	Thm (Ax2)
	10	$x+Su = S(x+u)$	US;9
	11	$y+Su = S(y+u)$	US;9
8	12	$S(x+u) = S(y+u)$	E:8,10,11
	13	$\forall x\forall y(Sx=Sy \longrightarrow x=y)$	Thm (Ax7)
	14	$S(x+u) = S(y+u) \longrightarrow x+u=y+u$	US:13
7,8	15	$x=y$	E+T:8,10,11,14,7
P(Su):			
7	16	$x+Su=y+Su \longrightarrow x=y$	D:15
	18	$P(u) \longrightarrow P(Su)$	D:16
	19	$\forall u(P(u) \longrightarrow P(Su))$	UG:18
	20	$\forall uP(u)$	T:1,6,19
	21	$\forall x\forall y\forall uP(u)$	UG:20

[3] $u+v=0 \longrightarrow u=0 \wedge v=0$.

Assume $u+v=0$, to prove $v\stackrel{?}{=}0$. By [1], if $v\neq 0$, then $v=Sy$ for some y . But then $u+v=u+Sy=S(u+y)\neq 0$ by Ax6. Therefore, $v=0$ must hold. Then, $u=u+0=u+v=0$, and $u=0$ too.

Formal: omitted.

[4] We prove
1. $\leq$ is reflexive,
2. $\leq$ is transitive,
3. $\leq$ is antisymmetric,
4. $\leq$ is dichotomous.

1. $x\stackrel{?}{\le}x$: $x\le x \underset{\text{def}}{\iff} \exists u.x+u=x$; but RHS is true, with $u=0$ (Ax1)

2. $x\le y \wedge y\le z \overset{\text{see Ax8}}{\overset{?}{\Longrightarrow}} x\le z$. Assume $x\le y$ & $y\le z$. That is (Ax8), we have u and v such that $x+u=y$ & $y+v=z$. It follows that $(x+u)+v=z$, and by Thm1, that $x+(u+v)=z$, Therefore, $w=u+v$ witnesses that $\exists w.x+w=z$, that is, $x\le z$. □

3. $x\le y \wedge y\le x \stackrel{?}{\Longrightarrow} x=y$. Assume $x\le y$ and $y\le x$, that is, the existence of u and v such that $x+u=y$ and $y+v=x$. But then $(x+u)+v=x$, and (Thm1), $x+(u+v)=x=x+0$. By cancellation, $u+v=0$. By [3], $u=v=0$; $y=x+u=x+0=x$. □

4. $x\le y \stackrel{?}{\vee} y\le x$. Induction on x .

Basis: $x=0$: $\overset{?}{\overline{0\le y \vee y\le 0}}$. Yes, since $0\le y$; this is because $0\le y \iff \exists u.0+u=y$, for which $u=y$ works, since $0+y=y+0=y$ (see Thm2, Ax1).

Induction step: Assume $x\le y$ or $y\le x$ (induction hypothesis), to show

$$Sx\le y \vee y\le Sx \qquad (1) \qquad ?$$

Case 1: $x \leq y$. There is u : $y=x+u$. We apply [1] to u .

Case 1.1 $u=0$. Now $y=x$, and $y=x \leq Sx=x+1$ (see L4); 2nd alternative holds in (1)

Case 1.2 $u=Sv=v+1$; now, $y=x+u=x+(v+1)=x+(1+v)=(x+1)+v=Sx+v$; which means that $Sx \leq y$: 1st alternative in (1).

Case 2. $y \leq x$, Then $y \leq x \leq Sx(=x+1)$, and by transitivity of $\leq$, $y \leq Sx$: 2nd alternative in (1).

□

[5] $x \leq y+1 \iff x \leq y \vee x=y+1$ (2)

1. $\Longrightarrow$: Assume $x \leq y+1$. $y+1=Sy=x+u$ for some u . Use [1] on u . Either $u=1$, or $u=v+1$ (s0me v). In the first case, $y+1=x$, thus @nd alternative in (2) holds. In the second case, $y+1=x+v+1$, thus $Sy=S(x+v)$, and $y=x+v$ by Ax2, that is, $x \leq y$: 1st alternative in (2).

□

We abbreviate $x \leq y \wedge x \neq y$ by $x<y$.

[6] (i) WOP: $\forall n[\forall k(k<n \to P(k)) \longrightarrow P(n)] \longrightarrow \forall n P(n)$

(ii) LNP: $(\exists x Px) \longrightarrow \exists u(Pu \wedge \forall v(Pv \to u \leq v))$

(iii) GNP: $\forall N[(\exists k P(k) \wedge \forall k(P(k) \to k<N)) \longrightarrow (\exists n P(n) \wedge \forall k(P(k) \to k \leq n))$.

[7] (i) WOP proved in PA (informally): We have $P \subseteq \mathbb{N}$ given, and we assume that

$$\forall n[\forall k(k<n \to P(k)) \longrightarrow P(n)] \qquad (*)$$

to prove

$$\forall n P(n) \quad .$$

In order to do this, we show

Lemma Under the assumption (*), we have

$$\forall n(k<n \to P(k)) \ . \qquad ?$$

Once we have done the Lemma, we apply it to Sn in place of n , and since $n<Sn$, we will have $P(n)$ as desired. Therefore, it is enough to prove the Lemma.

Proof of the Lemma: by ordinary induction (MI).

Basis: $n=0$: The assertion is $\forall n(k<0 \to P(k))$. Vacuously true, since $k<0$ is always false.

Induction step. Assume

$$\forall n(k<n \to P(k)) \ , \qquad (3)$$

to prove

$$\forall n(k<Sn \to P(k)) \quad . \qquad ??$$

To do so, assume $k<Sn(=n+1)$, to prove

$$P(k) \ . \qquad ???$$

$k<Sn$ says $k \leq Sn$ and $k \neq Sn$. By [5] , this implies $k \leq n$. But then either $k<n$ (Case 1), or $k=n$ (Case2) (since $\leq$ is the reflexive version of $<$). In the first case, by (3), we have $P(k)$.

Having done "Case 1", we have proved that

$$\forall k(k<n\rightarrow P(k))\ .$$

The initial assumption (*) above now says that $P(n)$ follows. That is, $P(k)$ is true in Case 2 ($k=n$) too. Thus, ??? , ?? , ? are all proved (in that order), and we are done.

(ii) LNP: proof is in the brackets [...] on p. 187 (Section 6.2)
(iii) GNP: proof is, essentially, in the Section 6.2; starts on last line, p. 187.

[8] $x\neq 0\longrightarrow(y\mid x\longrightarrow y\leq x)$ (*)

Lemma. $y\neq 0\longrightarrow x\leq x\cdot y$. Proof of lemma: Assume $y\neq 0$. By [1], $y=Su$, some u . $x\cdot y=x\cdot Su\underset{\substack{\uparrow\\ \text{Ax4}}}{=}x\cdot u+x\underset{\substack{\uparrow\\ \text{Thm2}}}{=}x+x\cdot u$; this shows that $x\leq x\cdot y$ (Ax8). □Lemma.

To prove (*), assume $x\neq 0$; to prove $y\mid x\longrightarrow y\leq x$, assume $y\mid x$, to prove $y\leq x$. By $y\mid x$, we have $x=y\cdot u$, some u . Since $x\neq 0$, we have $u\neq 0$. Therefore, by Lemma, $y\leq y\cdot u=x$ as desired.

[9] $\mid$ is a reflexive order.

$\mid$ is reflexive: $x\mid x$ since $x=x\cdot 1$ (L5,Thm5).

$\mid$ is transitive: assume $x\mid y\ \&\ y\mid z$, to show $x\overset{?}{\mid}z$. The assumptions give (Ax9) $y=x\cdot u$ and $z=y\cdot v$, hence, $z=(x\cdot u)\cdot v\underset{\substack{\uparrow\\ \text{Thm4}}}{=}x\cdot(u\cdot v)$; $z=x\cdot w$ for $w=u\cdot v$; $x\mid z$ (Ax9)

$\mid$ is antisymmetric: $x\mid y\ \&\ y\mid x\overset{?}{\Longrightarrow}x=y$. Assume $x\mid y\ \&\ y\mid x$. **Case 1** $x=0$. Then, by $x\mid y$, $y=x\cdot u$ (some u), and so $y=0\cdot u=0$ (L3), and $x=y=0$ as desired. Case 2: $x\neq 0$. Therefore, also $y\neq 0$ (since otherwise $y\mid x$, $x=y\cdot v$, gives $x=0$). By $x\mid y$ and $x\neq 0$, we have $x\leq y$ by [8] . Similarly, since x and y play symmetric roles in the theorem to be proved, we can show $y\leq x$. By the fact that $\leq$ is a reflexive order, hence antisymmetric, we conclude that $x=y$. □

[10] $(x\mid y\wedge x\mid(y+1))\longrightarrow x=1$.

Assume $x\mid y$ and $x\mid(y+1)$. We have u and v for which $y=x\cdot u$ and $y+1=x\cdot v$. Thus

$$x\cdot u+1=x\cdot v=x\cdot v+0. \qquad (1)$$

We have either $u\leq v$ (Case 1) or $v\leq u$ (Case 2) (see [4]).

But Case 2 is impossible: it would mean $u=v+w$,

$$x\cdot u+1=x\cdot(v+w)+1=(x\cdot v+x\cdot w)+1=x\cdot v+(x\cdot w+1)$$

which, together with (1), and [2] (cancellation) with Thm2 (commutativity), would give $x \cdot w+1=0$, false by (L4 and) Ax6.

Case 1 remains the only possibility; $v=u+w$ some w . From (1), $x \cdot u+1=x \cdot (u+w)=x \cdot u+x \cdot w$; by [2] and Thm2, $1=x \cdot w$. By [8], since $x\neq 0$, we get $x\leq 1$, $1=x+s$; and by [1], $x=Sz=z+1$, some z . Thus, $1=z+1+s$; by Thm1, Thm2, [2], $z+s=0$; by [3], $z=s=0$. Thus, $x=z+1=1$. Done.

[11] $(y\neq 0 \wedge y\neq 1) \longrightarrow \exists z(Pr(z) \wedge z \mid y)$. Assume $y\neq 0$ and $y\neq 1$. We apply the LNP (see [6] above),

$$(\exists x Px) \longrightarrow \exists u(Pu \wedge \forall v(Pv \rightarrow u\leq v)) \tag{1}$$

to the statement

$$P(x) :=: \qquad x \mid y \wedge x\neq 1 .$$

□ϕ⸢○ϱϕ $\exists x P(x)$: indeed, $x=y$ works since $y \mid y$ ([9]) and $y\neq 1$ (assumption). By (1), we have some u such that Pu and

$$\forall v(Pv \rightarrow u\leq v) . \tag{2}$$

Since Pu , we have $u \mid y$ and $u\neq 1$. We claim

$$u \text{ is a prime } \equiv Pr(u) \equiv \forall v(v \mid u \longrightarrow v=1 \vee v=u) \qquad (3)(?)$$

To prove (2), assume $v \mid u$, to show $v=1 \vee v=u$ (??); that is, assuming $v\neq 1$, we want $v=u$ (???). But by $v \mid u \mid y$, we have $v \mid y$ ([9]), and together with $v\neq 1$, Pv . By (2) and Pv , we have $u\leq v$. Since $v \mid u$ and $u\neq 0$ (because $u \mid y\neq 0$ (!)), by [8], we have $v\leq u$. $u\leq v \& v\leq u$ gives ([2]) $u=v$ as desired.

In conclusion: we found u such that $u \mid y$ and $Pr(u)$. □

[12] $\forall x\exists y(y\neq 0 \wedge \forall u((u\leq x \wedge u\neq 0) \longrightarrow u \mid y))$

By induction on x .

Basis: $x=0$. $y=1=S0$ now works since $(u\leq x \wedge u\neq 0) \Longrightarrow \perp$ (condition on y is vacuous).

Induction step: Suppose, with x arbitrary, that

$$\exists y(y\neq 0 \wedge \forall u((u\leq x \wedge u\neq 0) \longrightarrow u \mid y))$$

(*induction hypothesis*). Let y be such that

$$y\neq 0 \wedge \forall u((u\leq x \wedge u\neq 0) \longrightarrow u \mid y) . \tag{1}$$

Let $z=y \cdot (Sx)$, I **claim** that z is appropriate for

$$z\neq 0 \wedge \forall u((u\leq Sx \wedge u\neq 0) \longrightarrow u \mid z) \qquad (?)$$

$z=y\cdot(Sx)\neq 0$ since $y\neq 0$ and $Sx\neq 0$ (Ax6) [there should be a Lemma that says $u\neq 0\&v\neq 0 \Longrightarrow u\cdot v\neq 0$]

Assume $u\leq Sx \wedge u\neq 0$. By [5], $u\leq Sx$ implies $u\leq x$ (Case 1), or $u=Sx$ (Case 2). In Case1, by (1), $u\,|\,y$, and since $y\,|\,z$, by definition of z , we have $u\,|\,z$ as required for (?). In Case 2, again, $u\,|\,z$. □

[13] $\forall x\exists z(Pr(z)\wedge x\leq z)$

Let x be any number. By [12], there is y such that $y\neq 0 \wedge \forall u((u\leq x \wedge u\neq 0)\longrightarrow u\,|\,y)$. By [11], let z be such that $Pr(z) \wedge z\,|\,(y+1)$. Since $z\,|\,(y+1)$, and $Pr(z)$ (and thus $z\neq 1$), by [10], we have that $\neg(z\,|\,y)$. But for all u such that $u\leq x \wedge u\neq 0$, we have $u\,|\,y$. Therefore, $\neg(z\leq x \wedge z\neq 0)$. We also know that $z\neq 0$ since $Pr(z)$. Therefore, $\neg(z\leq x)$, and thus, by [4], we have $x\leq z$. We have both $Pr(z)$ and $x\leq z$. Done.

[14] $\forall a\forall b(0<b\longrightarrow\exists r\exists q(a=q\cdot b+r \wedge r<b)$

Proof. Assume $0<b$. By induction on a , we prove

$$\exists r\exists q(a=q\cdot b+r \wedge r<b) .$$

Basis: $a=0$: now, $q=r=0$ work ($0<b$).

Induction step: assume we have r and q such that

$$a=q\cdot b+r \wedge r<b \qquad (1)$$

(induction hypothesis). to show the existence of Q and R such that

$$a+1=Q\cdot b+R \wedge R<b . \qquad (2)\ (?)$$

Of course, from (1), we have

$$a+1=q\cdot b+(r+1) . \qquad (3)$$

Thus, if we have $r+1<b$ (Case 1), then we are done: $Q=q$ and $R=r+1$. It remains to consider the possibility that $\neg(r+1<b)$ (Case 2).

In Case 2: we know that $r<b$, which means that $b=r+s$, and $s\neq 0$ (otherwise we would have $b=r$). Thus, $s=t+1$, some t . $b=r+t+1=r+1+t$. If here $t\neq 0$, then $r+1<b$, which we assumed not to be the case. Therefore, $t=0$, and we conclude $b=r+1$. (In the last couple of lines, we inferred from $r<b$ and $\neg(r+1<b)$ that $r+1=b$, which looks a fairly obvious step ...)

From (3) and $b=r+1$, we conclude that $a+1=q\cdot b+b=(q+1)\cdot b$. But then, (2) holds with $Q=q$ and $R=0$ ($0<b$!). □

[15] $\forall a\forall b\exists d.GCD(a,b,d)$

Proof: By the WOP (see [6] above). More precisely, we prove the following statement by the WOP on the variable a :

$$P(a) \equiv \forall b(b<a\longrightarrow\exists d.GCD(a,b,d)) . \qquad (1)$$

We note that this will be enough. Namely, if $b=a$, then $GCD(a,a,a)$, as is easily seen, that is $d=a$ works. If, on the other hand, $b>a$, then $GCD(a,b,d)$ iff $GCD(b,a,d)$ as is easily seen, and thus we are back in the case " $a<b$ ".

Reminder: the WOP says

$$\forall a[\forall k(k<a \rightarrow P(k)) \longrightarrow P(a)] \longrightarrow \forall a P(a) \tag{2}$$

For our P in (1), we prove

$$\forall k(k<a \rightarrow P(k))) \longrightarrow P(a) \qquad (?)$$

("induction step according to the WOP"). Thus, we assume

$$\forall k(k<a \rightarrow P(k))) , \tag{3}$$

to prove

$$P(a) . \qquad (??)$$

Therefore, we let $b<a$, and try to show that there is d with $GCD(a,b,d)$. If $b=0$, there is no problem: $GCD(a,0,0)$ as is easily seen. Assume $0<b$. But then we have $\exists q \exists r(a=q \cdot b+r \wedge r<b)$; take such q and r ($r=a \bmod b$).

Lemma $\forall d(GCD(a,b,d) \Longleftrightarrow GCD(b,r,d))$

Proof of Lemma: use Ax13 (definition of $GCD(-,-)$); the proof is easy.

We have that $b<a$, and so, by (3), we have $P(b)$, Since $r<b$, we have some d such that $GCD(b,r,d)$. By the last lemma, $GCD(a,b,d)$. We have thus proved (??), and therefore also (?). By (2), we have $\forall a P(a)$; and as we noted before, this suffices.

[16] $\forall a \forall b \exists u \exists v \exists \hat{u} \exists \hat{v}.\ gcd(a,b)+\hat{u} \cdot a+\hat{v} \cdot b=u \cdot a+v \cdot b$.

Proof: similar to that of [15]; in fact, it is an extension of the proof of [15]. The statement is the same as

$$\forall a \forall b \exists u \exists v \exists \hat{u} \exists \hat{v} \exists d\ GCD(a,b,d) \wedge d+\hat{u} \cdot a+\hat{v} \cdot b=u \cdot a+v \cdot b \ .$$

Instead of proving

$$P(a) \ \equiv\ \forall b(b<a \longrightarrow \exists d.GCD(a,b,d))$$

by WOP, we prove

$$Q(a) \ \equiv\ \forall b(b<a \longrightarrow \exists d.(GCD(a,b,d) \wedge \exists u \exists v \exists \hat{u} \exists \hat{v}(d+\hat{u} \cdot a+\hat{v} \cdot b=u \cdot a+v \cdot b)) .$$

The details are omitted.

[17] $\forall p \forall a \forall b((\Pr(p) \wedge p \mid a \cdot b) \longrightarrow (p \mid a \vee p \mid b)$.

"Standard" algebra proof, using [16]. Assume $\Pr(p) \wedge p \mid a \cdot b)$, to prove

$$p \mid a \vee p \mid b \, . \qquad (1)$$

Let $d=\gcd(p,b)$. Since $d \mid p$, we must have either $d=1$ or $d=p$. If the second alternative holds, then $d=p \mid b$, and (1) is done. In the first case, using [16] , we have

$$1+\hat{u} \cdot b+\hat{v} \cdot p=u \cdot b+v \cdot p \, .$$

Multiplying with a , we get

$$a+\hat{u} \cdot a \cdot b+\hat{v} \cdot ap=u \cdot a \cdot b+v \cdot ap \, . \qquad (2)$$

Lemma If $a+p \cdot r=p \cdot s$, then $p \mid a$.

In effect, we used essentially this in [10]; I omit the easy proof.

The Lemma applies to (1), since, by assumption $p \mid a \cdot b$, the LHS in (1) is of the form $a+p \cdot r$, and the RHS is of the form $p \cdot s$. We conclude that $p \mid a$, and (1) is proved again.