Notes and Assignment 6/MATH 318/Fall, 2007
Due: Friday, November 30

For reference:
A list of all *Ax*ioms and certain *L*emmas and *Th*eore*m*s of Peano Arithmetic

Each statement in the list should be understood with all free variables bound by universal quantifiers in front. For instance, Ax1 is really $\forall x.x+0=x$, Ax2 is $\forall x \forall y.x+Sy=S(x+y)$.

*Ax*1. $x+0=x$
*Ax*2. $x+Sy=S(x+y)$
*Ax*3. $x \cdot 0=0$
*Ax*4. $x \cdot Sy=x \cdot y+x$
*AxSc*5. (*MI*; an *Ax*iom *Sc*heme)
$(P(0) \wedge \forall x(P(x) \longrightarrow P(Sx))) \longrightarrow \forall x P(x)$
*Ax*6. $Sx \neq 0$
*Ax*7. $Sx=Sy \longrightarrow x=y$

*Thm*1. $(x+y)+z=x+(y+z)$
*L*1. $0+x=x$
*L*2. $S(x+y)=Sx+y$
*Thm*2. $x+y=y+x$
*Thm*3. $x \cdot (y+z)=(x \cdot y)+(x \cdot z)$
*Thm*4. $(x \cdot y) \cdot z=x \cdot (y \cdot z)$
*L*3 $0 \cdot x=0$
*L*4. $x+1=Sx$ [1 abbreviates S0]
*L*5 $1 \cdot x=x$
*L*6 $(x+y) \cdot z=x \cdot z+y \cdot z$
*Thm*5. $x \cdot y=y \cdot x$

(*End of List*).

The numbered problems that follow, with the obvious exceptions of [6] and [7], should be understood with a phrase like "**Prove** (**that**) ..." prefixed to them. They are all meant with universal quantifiers in front binding all variables, if any, that are now free in the statement. All variables range over $\mathbb{N}=\{0, 1, 2, 3, ...\}$, the set of non-negative integers.

Unless otherwise stated, each proof asked for here should be given in an informal style, but so that the proof could be turned into a formal deduction relatively easily.

In all the proofs, ultimately, only the axioms of Peano Arithmetic are to be used. But of course, in each case, theorems proved previously may and should always be used as much as possible. In particular, all results (axioms, lemmas and theorems) in the above list may be used. Also, the result of [k] can be used in doing [ℓ] if k<ℓ even if you do not do [k].

There are axioms Ax8, Ax9, ... introduced later below. They are all *explicit definitions* of new terms introduced by them. They can be *eliminated*: all theorems using them can be equivalently restated and proved without them, albeit in a longer way.

It is sometimes useful to formulate and prove a *lemma* (auxiliary theorem), to be used in the main proof (or even in another lemma ...). For instance, think of usual porperties of the order:

$a \le b \implies a+c \le b+c$,
$a \le b \implies a \cdot c \le b \cdot c$;

they are likely to be useful for some of the theorems.

When a formal proof is asked for, a deduction of entailment of the form $PA \vdash \Phi$ (in Extended Natural Deduction) is meant, with PA meaning the set of all axioms of PA. In such deductions, any line of the form $PA \vdash \Gamma$ where Γ is already known to have been proved is allowed with the annotation "theorem" (or "Ax3", if Γ is Ax3 ...) .

One final note: in problem [10], and in some of the latest ones, one has to circumvent the difficulty that we don't have subtraction or negative numbers. For instance, consider this: suppose that $a \mid b$ and $a \mid c$, and we also have that $b+d=c$. Then, of course, $a \mid d$, since $d=c-a=\hat{c} \cdot b - \hat{a} \cdot b = (\hat{c}-\hat{a}) \cdot b$. How do we do this proof without explicit subtraction? We use the definition and properties of the order $\le$, and also use cancellation. In the present case, we show that we must have $\hat{a} \le \hat{c}$, and thus $\hat{c}-\hat{a}$ is well-defined, and then that $d=(\hat{c}-\hat{a}) \cdot b$.

[1] $x=0 \vee \exists y.x=y+1$. **Also give a formal proof**.

[2] *Law of cancellation*: $x+u=y+u \implies x=y$. **Also give a formal proof.**

[3] $u+v=0 \implies (u=0 \wedge v=0)$. **Also give a formal proof.**

We introduce the "less-than-or-equal" relation $\le$ by a definition that we adopt as a new axiom:

*Ax*8 $\quad \forall x \forall y (x \le y \longleftrightarrow \exists u (x+u=y))$.

[4] $\le$ is a total reflexive order on $\mathbb{N}$.

[5] $x \le y+1 \iff x \le y \vee x=y+1$.

[6] Write down
(i) the *Well Ordering Principle* (WOP) (see Notes, pp 183, 184);
(ii) the Least *Least Number Principle* (LNP) (p 187); and
(iii) the Least *Greatest Number Principle* (GNP) (pp 187, 188).
Use the new unary relation-symbol P to talk about a(n arbitrary) subset of $\mathbb{N}$, and use the predicate-symbol $\le$. Write the statements in the form of sentences (no free variables) in predicate logic; do not use a quantifier $\forall P$ on P .

[7] Prove (in Peano Arithmetic) the WOP, the LNP and the GNP, in that order. You may follow the outlines starting on the bottom of page 186, ending on page 188. In the case the GNP, there is a better proof than the one in the Notes: note that "x is maximal just in case $N-x$ is minimal".

We introduce further definitions in the form of axioms: those of *divisibility*, and *prime number*.

*Ax*9 $\quad \forall x \forall y (x \mid y \longleftrightarrow \exists u.y=xu)$

*Ax*10 $\quad \forall x (\mathrm{Pr}(x) \longleftrightarrow (x \ne 1 \wedge \forall v (v \mid x \to (v=1 \vee v=x))))$

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

[9] The relation $\mid$ is a reflexive order on $\mathbb{N}$.

[10] $(x \mid y \wedge x \mid (y+1)) \longrightarrow x=1$.
(**Remark:** in usual arithmetic, this would use the equality $x(u-v)=xu-xv$. In our present context, we are not using subtraction (because it is not always defined within $\mathbb{N}$). You should circumvent this by using cancellation ([2] above), among other things.)

[11] $(y\neq 0 \wedge y\neq 1) \longrightarrow \exists z(\mathrm{Pr}(z) \wedge z \mid y)$

[12] For every x , there is $y\neq 0$ such that $\forall u((u\leq x \wedge u\neq 0) \rightarrow u \mid y)$.

[13] (**Euclid's theorem**: "there are infinitely many primes")
For every x , there is z such that $\mathrm{Pr}(z)$ and $x\leq z$.
(**Hint:** use [12], to get y as there; next, take $y+1$, and apply [11] to $y+1$, to get z .)

*Ax*11. $x<y \longleftrightarrow x\leq y \wedge x\neq y$.

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

*Ax*12. $0<b \longrightarrow \exists q.(a = q \cdot b + a\mathrm{mod}b \wedge a\mathrm{mod}b < b)$
*Ax*13. $\mathrm{GCD}(a, b, d) \longleftrightarrow \forall c(c \mid d \longleftrightarrow (c \mid a \wedge c \mid b))$

[15] $\forall a \forall b \exists d.\mathrm{GCD}(a, b, d)$
Hint: see p.156 in the Notes.

*Ax*14. $\gcd(a, b)=d \longleftrightarrow \mathrm{GCD}(a, b, d)$

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

[17] $\forall p \forall a \forall b((\mathrm{Pr}(p) \wedge p \mid ab) \longrightarrow (p \mid a \vee p \mid b))$