## Problem Set 1

## Solutions

## Foundations of Number Theory

Math 435, Fall 2006

1. (20 pts.) Put $a_{n}:=n^{3}+2 n$ and $b_{n}:=5^{2 n}-1$ for every $n \in \mathbb{N}, n \geq 1$. We show $3 \mid a_{n}$ and $24 \mid b_{n}$ for every $n \geq 1$, by induction on $n$. Base step: We have $a_{1}=3$ and $b_{1}=24$, so the claims hold trivially for $n=1$. Inductive step: Suppose we have shown $3 \mid a_{n}$ and $24 \mid b_{n}$ for a certain $n \geq 1$. We compute

$$
a_{n+1}=(n+1)^{3}+2(n+1)=n^{3}+3 n^{2}+5 n+3
$$

and thus

$$
a_{n+1}=a_{n}+3\left(n^{2}+n+1\right)
$$

Since $3 \mid a_{n}$, this yields $3 \mid a_{n+1}$. Similarly

$$
b_{n+1}=5^{2(n+1)}-1=5^{2 n} \cdot 25-1=\left(5^{2 n}-1\right) \cdot 25+25-1=b_{n}+24
$$

and $24 \mid b_{n}$ yields $24 \mid b_{n+1}$.
2. (10 pts.) We proceed by induction on $n=1,2, \ldots$ Base step: If $n=1$, then $(1+x)^{1} \geq 1+1 \cdot x$ for all $x \in \mathbb{R}$. Inductive step: Suppose the claim holds for $n$, and we want to show it for $n+1$ in place of $n$. That is, we want to show $(1+x)^{n+1} \geq 1+(n+1) x$ if $1+x>0$. Now by inductive hypothesis and since $1+x>0$, we have

$$
(1+x)^{n+1}=(1+x)^{n}(1+x) \geq(1+n x)(1+x)
$$

But
$(1+n x)(1+x)=1+n x+x+n x^{2}=1+(n+1) x+n x^{2} \geq 1+(n+1) x$, since $n x^{2} \geq 0$.
3. (20 pts.) For $n \in \mathbb{N}$ we have $(2 n+1)^{2}=4 n(n+1)+1$ and $2 \mid n(n+1)$; hence $(2 n+1)^{2}$ has remainder 1 upon division by 8 . Now suppose $m, n \in \mathbb{Z}$ are odd; then $m^{2}=8 a+1$ and $n^{2}=8 b+1$ for some $a, b \in \mathbb{Z}$, hence $(m+n)(m-n)=m^{2}-n^{2}=8(a-b)$ is divisible by 8 .
4. (10 pts.) The mistake is simply that in the inductive step, after taking out the two cats, there might not be any cats left: if $n=1$, then we are left with no cats at all, so it is meaningless to say that this "rest of the set has $n-1$ cats of color $x$." So we cannot conclude that the first cat must have color $x$ as well. The moral of the story is: in proving the inductive step $n \rightarrow n+1$, we have to be careful and make sure that the proof applies to all $n \geq 1$. (Or $n \geq k$, if we start the induction at $k$, say.)
5. (20 pts.) We proceed by induction on $n=1,2, \ldots$ Base step: If $n=1$, then

$$
1^{2}=1=\frac{1}{6} 1(1+1)(2 \cdot 1+1) .
$$

Inductive step: Suppose the statement holds for $n$ :

$$
1^{2}+2^{2}+\cdots+n^{2}=\frac{1}{6} n(n+1)(2 n+1)
$$

and we we want to show that it holds for $n+1$. That is, we want to show:

$$
1^{2}+2^{2}+\cdots+(n+1)^{2}=\frac{1}{6}(n+1)(n+2)(2(n+1)+1)
$$

We compute that

$$
\frac{1}{6} n(n+1)(2 n+1)=\frac{1}{3} n^{3}+\frac{1}{2} n^{2}+\frac{1}{6} n
$$

and

$$
\frac{1}{6}(n+1)(n+2)(2(n+1)+1)=\frac{1}{3} n^{3}+\frac{3}{2} n^{2}+\frac{13}{6} n+1
$$

By inductive hypothesis and using these equalities, we get:

$$
\begin{aligned}
1^{2}+2^{2}+\cdots+(n+1)^{2} & =\left(1^{2}+2^{2}+\cdots+n^{2}\right)+(n+1)^{2} \\
& =\frac{1}{3} n^{3}+\frac{1}{2} n^{2}+\frac{1}{6} n+(n+1)^{2} \\
& =\frac{1}{3} n^{3}+\frac{1}{2} n^{2}+\frac{1}{6} n+n^{2}+2 n+1 \\
& =\frac{1}{3} n^{3}+\frac{3}{2} n^{2}+\frac{13}{6} n+1 \\
& =\frac{1}{6}(n+1)(n+2)(2(n+1)+1)
\end{aligned}
$$

6. (20 pts.) There are $\frac{1}{2} n(n+1)+1$ many regions. We prove this by induction on $n$. For $n=1$ lines, there are $2=\frac{1}{2} 1(1+1)+1$ regions. If we have $n$ lines, and we add another one, then we obtain $n+1$ new regions. (Draw a picture for $n=1,2,3,4!$ ) So we have $\frac{1}{2} n(n+1)+1+(n+1)=\frac{1}{2}(n+1)(n+2)+1$ regions.
7. (20 pts. extra credit.) Let $n \geq 1$ be a natural number. For every $k \geq 1$ let $f_{k}$ be the remainder of $F_{k}$ upon division by $n$, so $0 \leq f_{k}<n$. Among the $n^{2}+1$ pairs $\left(f_{1}, f_{2}\right),\left(f_{2}, f_{3}\right), \ldots,\left(f_{m}, f_{m+1}\right)$, where $m=n^{2}+1$, there are two identical pairs (since only $n^{2}$ distinct pairs both of whose components come from $\{0, \ldots, n-1\}$ exist). Suppose $\left(f_{k}, f_{k+1}\right)=\left(f_{l}, f_{l+1}\right)$ with $1 \leq k<l \leq m$; choose $k$ minimal. One shows easily (check!) that $k>1$, since otherwise $\left(f_{k-1}, f_{k}\right)=\left(f_{l-1}, f_{l}\right)$, contradicting minimality of $k$. Hence $\left(f_{l}, f_{l+1}\right)=\left(f_{1}, f_{2}\right)=(1,1)$, so $F_{l-1}=F_{l+1}-F_{l}$ is divisible by $n$, and $1 \leq l-1 \leq n^{2}$.

Total: 100 pts. +20 pts. extra credit

