Ch 7

§1 **Prop**: The integer n is odd if and only if n^2 is odd

Prop: Let $a, b \in \mathbb{Z}$. Then $a \equiv b \bmod 6$ if and only if $a \equiv b \bmod 2$ and $a \equiv b \bmod 3$.

§2 **Theorem**: Let A be an $n \times n$ matrix. The following are equivalent:

(a) A is invertible
(b) $A\vec{x} = \vec{b}$ has a unique solution for all $\vec{b} \in \mathbb{R}^n$
(c) $A\vec{x} = \vec{0}$ has only the trivial solution
(d) The reduced row echelon form of A is I_n.
(e) $\det(A) \neq 0$
(f) 0 is not an eigenvalue of A

§3 Existence Theorems: $\exists x, R(x)$

To prove, just exhibit an example, or show an example exists.

Prop: There is an even prime number.

proof: 2 is prime and even □

Prop: There is an integer which can be written as the sum of two cubes in ~~two~~ different ways.

pf/ $1729 = 1^3 + 12^3 = 9^3 + 10^3$ □

Prop: If $a,b \in \mathbb{N}$, then there exists $k,\ell \in \mathbb{Z}$ such that $\gcd(a,b) = ak+b\ell$.

proof: Let $a,b \in \mathbb{N}$. Define $A = \{ax+by \mid x,y \in \mathbb{Z}\}$. Notice that A contains negative, and positive numbers, as well as 0:

$-a, a \in A$ and one is positive and one is negative (using $x=-1, y=0$ and $x=1, y=0$) and $0 \in A$ since $a(0)+b(0)=0$. Let d be the smallest positive element of A. Then

$$d = ak+b\ell, \text{ for some } k,\ell \in \mathbb{Z}.$$

Claim: $d = \gcd(a,b)$

By the division algorithm, we have

$$a = dq+r \text{ for } q,r \in \mathbb{Z},\ 0 \le r < d.$$

Then

$$r = a-dq = a-q(ak+b\ell) = a(1-qk)+b(-q\ell)$$

Therefore $r \in A$. But r is nonnegative, so if $r>0$, then $r \ge d$ since d is the smallest positive element of A. This contradicts the definition of r, therefore $r=0$. Thus $a=dq$ and we have $d \mid a$.

A similar proof shows that $d \mid b$ and so d is a common divisor of a and b. Thus $d \le \gcd(a,b)$.

(3)

Since $\gcd(a,b)$ divides a & b, we have $a = \gcd(a,b)\cdot m$ and $b = \gcd(a,b)\cdot n$. Thus

$$d = ak+bl = \gcd(a,b)\cdot m\cdot k + \gcd(a,b)\cdot n\cdot l$$
$$= \gcd(a,b)(mk+nl)$$

Thus $\gcd(a,b) \mid d$. Since d & $\gcd(a,b)$ are positive, this means $d \geq \gcd(a,b)$.

Therefore $d = \gcd(a,b)$. □

Thm: Let $a,b \in \mathbb{N}$. There exists a unique $d \in \mathbb{N}$ such that $m \in \mathbb{Z}$ is a multiple of d if and only if $m = ax+by$ for some $x,y \in \mathbb{Z}$.