Lecture 3

True or false:

If $7 \mid ab$ then $7 \mid a$ or $7 \mid b$.

True by Euclid's lemma since 7 is prime.

If $8 \mid a^2$, then $8 \mid a$.

False. Take $a=4$

If $22 \mid a^2$, then $22 \mid a$.

True. Both factors of 22 (2 and 11) are primes and it doesnt work w/ squares of prime factors.

DEF: If $\gcd(a,b)=1$, then a and b are coprime.

Problem: Let $a,b,x \in \mathbb{N}$. assume $\gcd(a,x)=1$, $\gcd(b,x)=1$

Prove $\gcd(ab,x)=1$

Solution: It suffices to prove that for every prime p, p is not a common divisor of ab and x.

Suppose by contradiction that prime p divides ab and also x.

Since $p \mid ab$, from Euclid's lemma, $p \mid a$ or $p \mid b$.

In the case $p \mid a$, $p \mid x$, contradicting $\gcd(a,x)=1$

In the case $p \mid b$, $p \mid x$, ... $\gcd(b,x)=1$

Bézout's Lemma: For every $a,b \in \mathbb{N}$, there exist $x,y \in \mathbb{Z}$ $\ni \gcd(a,b) = xa + yb$

Euclid's lemma: If p is prime and $p|ab$, then $p|a$ or $p|b$.

Proof using Bizout's:

Assume $p\nmid a$ and let us show $p|b$,

We claim that $\gcd(p,a)=1$. (Explanation if $d|p$ and $d|a$. then $d=1$ or $d=p$, but d cannot be p since $p\nmid a$, so $d=1$)

From Bizout's, $\exists x,y \in \mathbb{Z} \ni$

$$1 = xa + yp$$

$$b = xab + ypb$$

Since $p|ab$ and $p|ypb$, then $p|LHS$

Hence $p|b$.

Divisibillity Rules

Here is a divisibillity rule by 7. In base 10, remove the last digit, then subtract from the result double the last digit. The result is div. by 7 $\longleftrightarrow$ the original number is divisible by 7.

Ex. 441 $\quad 44 - 1\cdot 2 = 42 \checkmark$

Problem: Prove the rule works.

Solution: Take $n \in \mathbb{N}$. Write it as $10a+b$ where b is the units digit. $m = a - 2b$. We need to proove $7|n \leftrightarrow 7|m$

$10a+b = 7k$

attempt $\quad n - m = 9a + 3b$

$\quad 2n + m = 21a \checkmark$

Since $7|n$ and $7|2n+m$, $7|m$.