

```
Congruence mod n

example:

66666663 = 788253 (mod 10)

WHY?

66666663

_ 788253

XXXXXXXX

Congruence Mod n

example:

6666663 = 788253 (mod 10)

WHY?

66666663

Congruence Mod n

example:

66666663 = 788253 (mod 10)

WHY?

66666663

Congruence Mod n

example:

666666663

Congruence Mod n

example:

66666663

Congruence Mod n

examp
```

```
Remainder Lemma
a \equiv b \pmod{n}

iff
rem(a,n) = rem(b,n)

example: 30 \equiv 12 \pmod{9}

since
rem(30,9) = 3 = rem(12,9)

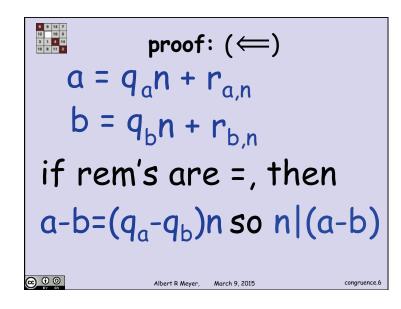
(30,9) = 3 = rem(12,9)

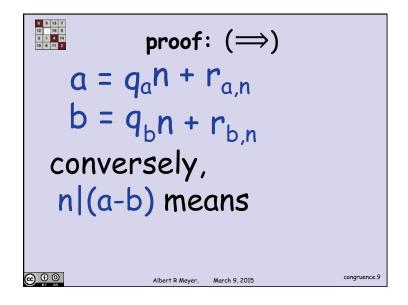
Albert R. March 9, 2015
(30,9) = 3 = rem(12,9)
```

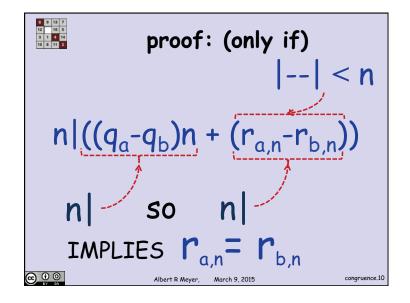
```
Remainder Lemma
a \equiv b \pmod{n}

iff
rem(a,n) = rem(b,n)

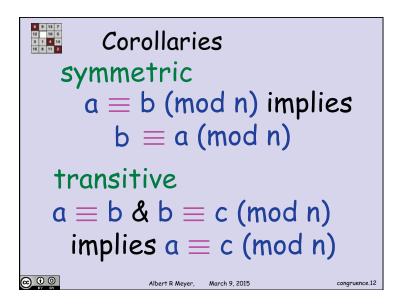
abbreviate: r_{b,n}
```

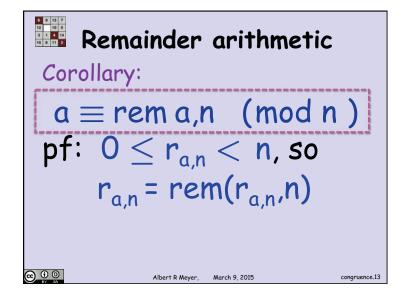


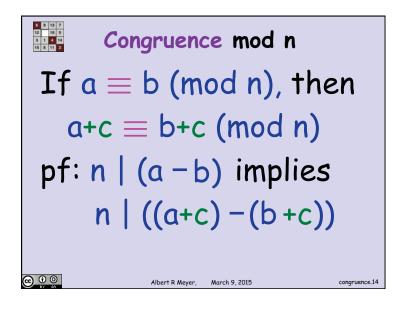




```
Remainder Lemma
a \equiv b \pmod{n}
iff
rem(a,n) = rem(b,n)
QED
Albert R Meyer, March 9, 2015 congruence.11
```







```
Congruence mod n

If a \equiv b \pmod{n}, then

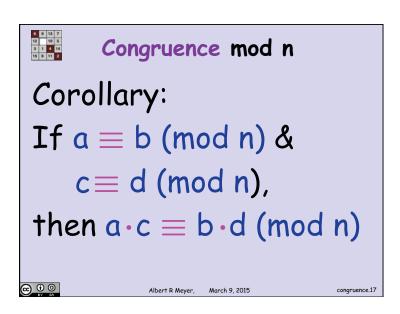
a \cdot c \equiv b \cdot c \pmod{n}

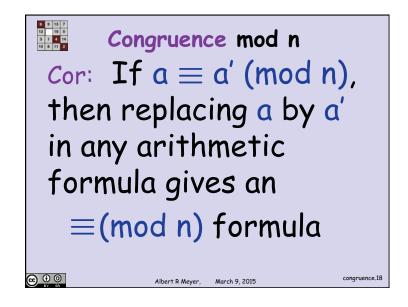
pf: n \mid (a - b) \text{ implies}

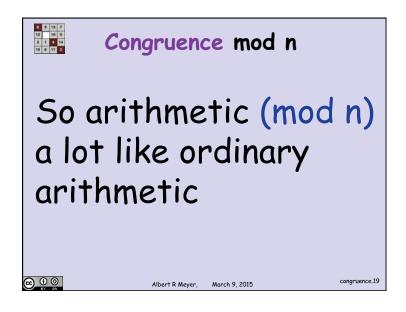
n \mid (a - b) \cdot c, and so

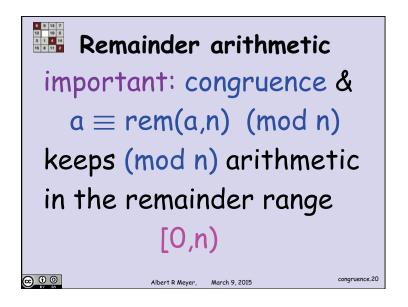
n \mid ((a \cdot c) - (b \cdot c))

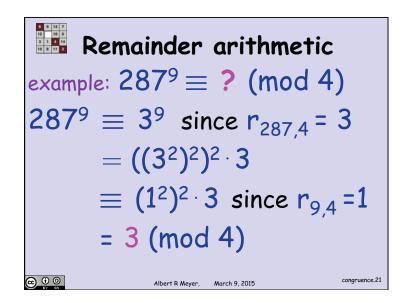
Albert R Meyer. March 9, 2015
```











MIT OpenCourseWare http://ocw.mit.edu

6.042J / 18.062J Mathematics for Computer Science Spring 2015

For information about citing these materials or our Terms of Use, visit: http://ocw.mit.edu/terms.