



4/2/08 2:20PM

```
inverses (mod n)

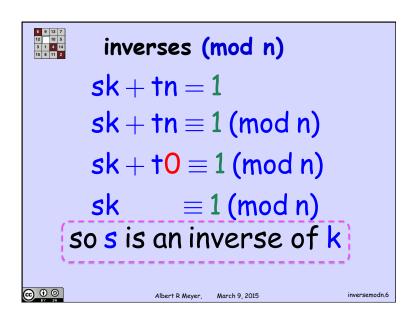
If gcd(k,n)=1, then have k'

k' \cdot k \equiv 1 \pmod{n}.

k' is an inverse mod n of k

pf: sk + tn = 1, so

just \ let \ k' be s
```



```
cancellation (mod n)

If a \cdot k \equiv b \cdot k (mod n)

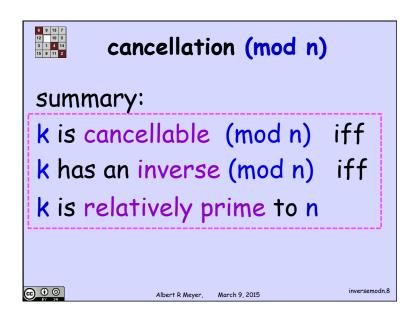
and gcd(k,n) = 1, then

multiply by k':

(a \cdot k) \cdot k' \equiv (b \cdot k) \cdot k' (mod n)

a \cdot 1 \equiv b \cdot 1

so a \equiv b \pmod{n}
```



4/2/08 2:20PM