

```
inverses (mod n)

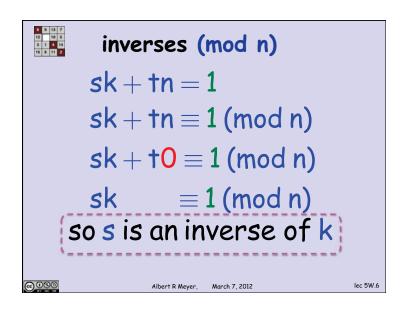
If gcd(k,n)=1, then have k'

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

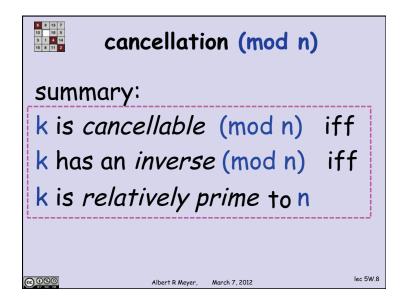
k' is an inverse mod n of k

pf: sk + tn = 1, so

just let k' be s
```



```
 \begin{array}{c} \textbf{cancellation (mod n)} \\ \textbf{If } a \cdot k \equiv b \cdot k \text{ (mod n)} \\ \textbf{and } \textbf{gcd(k,n)} = 1, \text{ then} \\ \textbf{multiply by k':} \\ \textbf{(} a \cdot k\textbf{)} \cdot k\textbf{'} \equiv \textbf{(} b \cdot k\textbf{)} \cdot k\textbf{'} \text{ (mod n)} \\ \textbf{a} \cdot 1 \equiv b \cdot 1 \\ \textbf{so} \quad \textbf{a} \equiv \textbf{b} \text{ (mod n)} \\ \textbf{Albert R. Meyer.} \quad \textbf{March 7, 2012} \end{array}
```



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.