```
Mathematics for Computer Science
MIT 6.042J/18.062J

Congruences:
arithmetic (mod n)
```

```
Congruence mod n

Def: a \equiv b \pmod{n}

iff n \mid (a - b)

example: 30 \equiv 12 \pmod{9}

since

9 divides 30 - 12
```

```
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)

Albert R. March 31, 2010

88.8
```

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

iff

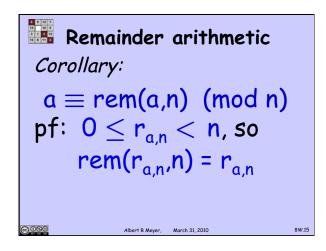
rem(a,n) = rem(b,n)

abbreviate: r_{b,n}
```

```
proof: (if)
a = q_a n + r_{a,n}
b = q_b n + r_{b,n}
if rem's are =, then
a-b=(q_a-q_b)n \text{ so } n|(a-b)
(only if) proof similar

Albert R Meyer. March 31, 2010 8W.11
```

```
Remainder Lemma
a \equiv b \pmod{n}
iff
rem(a,n) = rem(b,n)
QED
Albert R Meyer, March 31, 2010 6W.14
```



```
More Corollaries

• symmetric

a = b (mod n) implies

b = a (mod n)

• transitive

a = b & b = c (mod n)

implies a = c (mod n)
```

```
Congruence mod n

If a ≡ b (mod n), then

a+c ≡ b+c (mod n)

pf: n | (a - b) implies

n | ((a+c) - (b+c))
```

```
Congruence mod n

Corollary:

If a \equiv b \pmod{n} &

c \equiv d \pmod{n},

then a+c \equiv b+d \pmod{n}
```

```
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}

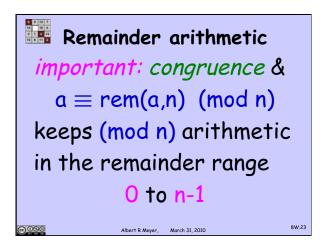
n \mid (a - b) \cdot c, and so

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

Albert R Meyer. March 31, 2010

8W.21
```

```
Congruence mod n
Cor: if a ≡ a' (mod n),
then replacing a by a'
in any arithmetic
formula gives an
≡ (mod n) formula
```



Remainder arithmetic example: $287^9 \equiv ? \pmod{4}$ $287^9 \equiv 3^9 \text{ since } r_{287,4} = 3$ $= ((3^2)^2)^2 \cdot 3$ $\equiv (1^2)^2 \cdot 3 \text{ since } r_{9,4} = 1$ $= 3 \pmod{4}$

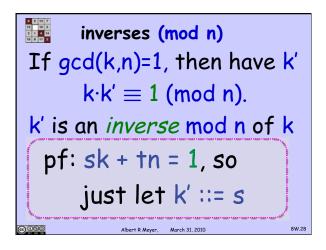
Congruence mod n
So arithmetic (mod n) a lot like ordinary arithmetic
the main difference:

8.2 = 3.2 (mod 10)

8 \neq 3 (mod 10)

no arbitrary cancellation

when can you cancel k?
--when k has no common factors with n



```
cancellation (mod n)

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

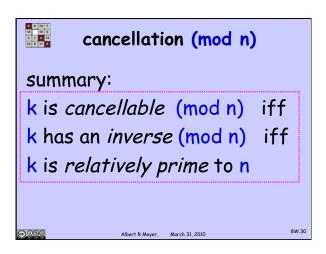
and gcd(k,n) = 1, then

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}
```



arithmetic mod a prime

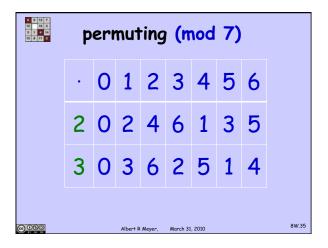
If p is prime & k not a multiple of p, can cancel k. So

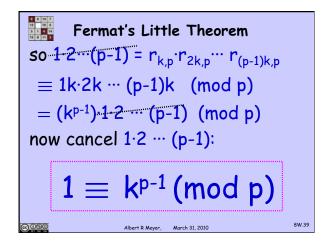
1·k, 2·k, ..., (p-1)·k

are all different (mod p).

So their remainders on division by p are all different.

arithmetic mod a prime, p
so if p does not divide k,
then multiplying
1, 2, ..., (p-1)
by k and taking remainders
just permutes them.





```
inverses (mod prime)

so kp-2 is a (mod p)

inverse of k

--an alternative to

finding inverses with

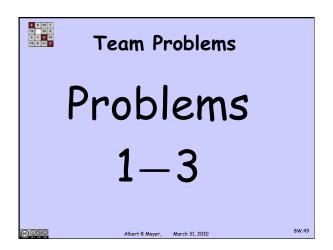
the pulverizer
```

```
Remainder arithmetic 28^{99885} \equiv ? \pmod{5} [r_{28,5} = 3]
```

```
Remainder arithmetic
3^{99885} \equiv ? \pmod{5}
= 3^{4\cdot q+rem(99885,4)}
= (3^{4})^{q} \cdot 3^{rem(99885,4)}
```

```
Remainder arithmetic
3^{99885} \equiv ? \pmod{5}
= 3^{4\cdot q+rem(99885,4)}
= (3^4)^q \cdot 3^{rem(99885,4)}
= (1)^q \cdot 3^{rem(99885,4)}
[Fermat]
```

```
Remainder arithmetic
3^{99885} \equiv 3 \pmod{5}
= 3^{4\cdot q + rem(99885, 4)}
= (3^{4})^{q} \cdot 3^{rem(99885, 4)}
\equiv (1)^{q} \cdot 3^{rem(99885, 4)}
\equiv 3^{rem(99885, 4)} = 3^{1}
Albert R Meyer. March 31, 2010
```



MIT OpenCourseWare http://ocw.mit.edu

6.042J / 18.062J Mathematics for Computer Science Spring 2010

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