

## Equivalence class modulo 3

- Reflexive:  $m T m \implies 3 \mid (m m) \implies 3 \mid 0$  which is true
- Symmetric: We must show that if m T n then n T m. By definition of the relation and divides, m T n ⇒ 3 | (m n). So there must exists a k such that 3k = (m n). If we multiply both sides by -1, then 3(-k) = n m. Let k' = -k, and 3k' = (n m) which means that 3 | (n m) and n T m.
- Transitive: We must show that if m T n and n T p then m T p. Using the same argument as before, if m T n and n T p there must exists r and s such that 3r = m n and 3s = n p. If we add those two equations, 3r + 3s = m n + n p, and then 3(r + s) = m p. Let k = (r + s), and we have 3k = (m p). So  $3 \mid (m p)$  and m T p.

Prof. Adam J. Aviv (GW)

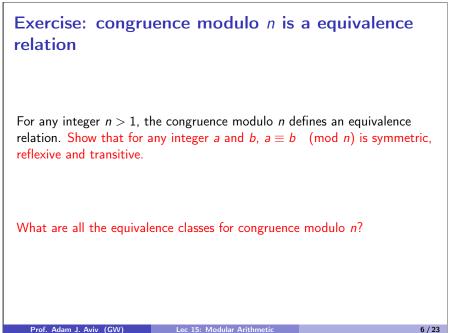
Lec 15: Modular Arithmetic

3 / 23

Modulo congruence
Definition
Let $m$ and $n$ be integers and let $d$ be a positive integer. We say that $m$ is congruent to $n$ modulo $d$ and write
$m\equiv n \pmod{d}$
if, and only if, $d \mid (m-n)$
More formally, $m\equiv n \pmod{d} \iff d \mid (m-n)$

Prof. Adam J. Aviv (GW)

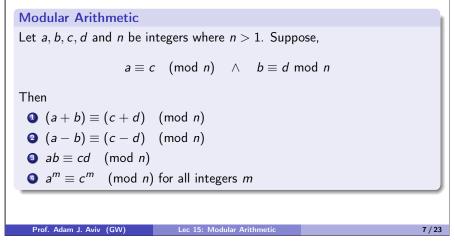
# **Modular Equivalences** If *a*,*b*, and *n* are integers with n > 1, we can desribe modular equivalence of a and b modulo n in any of the following ways: **1** $n \mid (a - b)$ 2 $a \equiv b \pmod{n}$ (or $a \equiv_n b$ ) $\exists k, a = b + kn$ **④** a and b have the same (non-negative) remainder when divided by n**(3)** $a \mod n = b \mod n$ Lec 15: Modular Arithmetic Prof. Adam J. Aviv (GW) 5/23



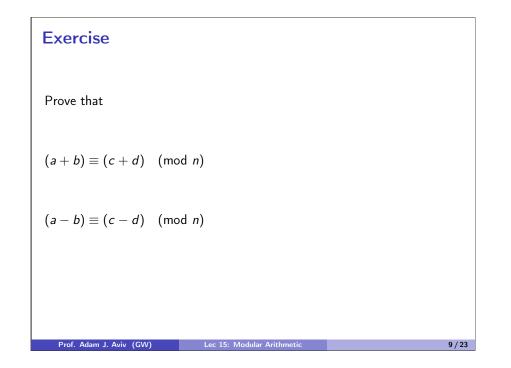
6/23

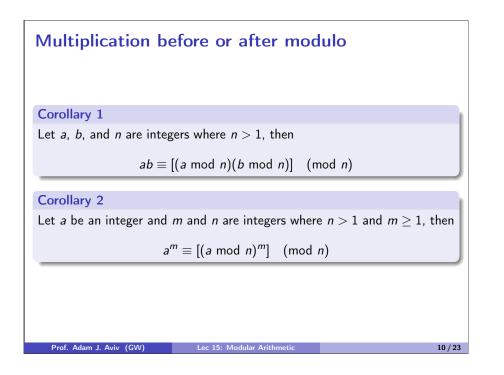
# **Modular Arithmetic**

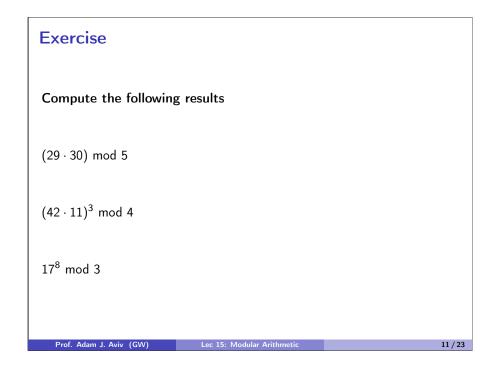
Modular arithmetic is performing standard operations (addition, subtraction, multiplication) under a modulo, and because of the small set of equivalence classes, there are some interesting properties.



Multiplication Equivalence         If $a, b, c, d$ and $n$ are integers with $n > 1$ and $a \equiv c \pmod{n}$ $h \equiv c \pmod{n}$ $h \equiv c \pmod{n}$ $h \equiv c \pmod{n}$	
then $ab \equiv cd \pmod{n}$	
Proof.	
If $a \equiv c \pmod{n}$ and $b \equiv_n d \pmod{n}$ then exists $r$ and $s$ such that $a = c + rn$ b = d + sn. So	and
ab = (c + rn)(d + sn)	
= cd + crn + rn + rnsn	
= cd + n(cr + r + rsn)	
Let $k = (cr + r + rsn)$ , so $ab = cd + nk$ . By definition of congruence modulo $n$ , $ab \equiv cd \pmod{n}$	







# **GCD: Greatest Common Denominator**

## Definition

The greatest common denominator (or GCD) of two positive integers *a* and *b* is largest integer value *n* such that  $n \mid a$  and  $n \mid b$ , and we would say that the gcd(a, b) = n

Euclid's algorithm for gcd(a, b):

- Check if b is 0, if it is, then gcd(a, 0) = a and we're done.
- 2 If b > 0, then let  $r = a \mod b$
- **③** Repeat (1), now computing gcd(b, r) (so a is b, and b is r)

```
Compute gcd(330, 156)
```

12 / 23

# Linear combination of integersDefinitionAn integer d is said to be a linear combination of integers a and b if, and<br/>only if, there exists integers s and t such that as + bt = d.Theorem (GCD as a Linear Combination)For all integers a and b, not both zero, if d = gcd(a, b), then there exists<br/>integers s and t such that as + bt = d.Print and t such that as + bt = d.

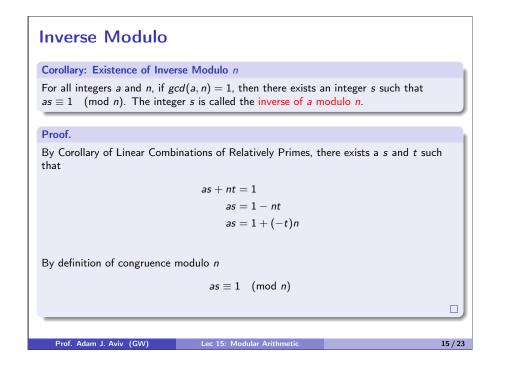
## **Relative Prime and Linear Combinations**

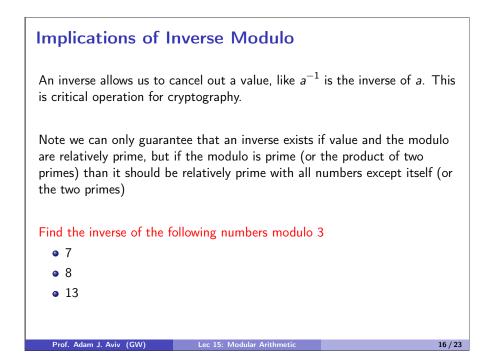
## Definition

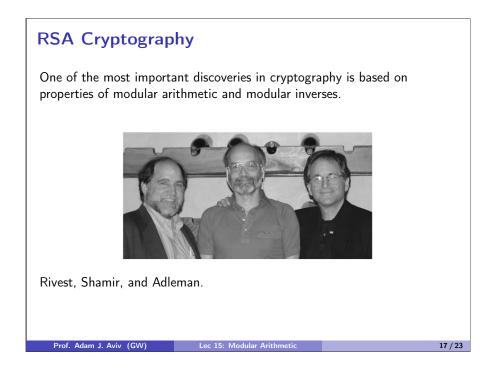
Two positive integers a and b are relatively prime if gcd(a, b) = 1. That is, they share no common divisors.

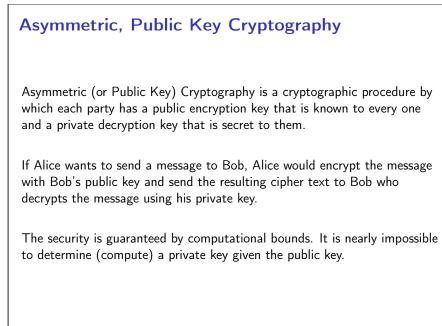
## **Corollary: Linear Combination of Relative Primes**

If a and b are relatively prime (that is gcd(a, b) = 1), then there exists integers s and t such that as + bt = 1



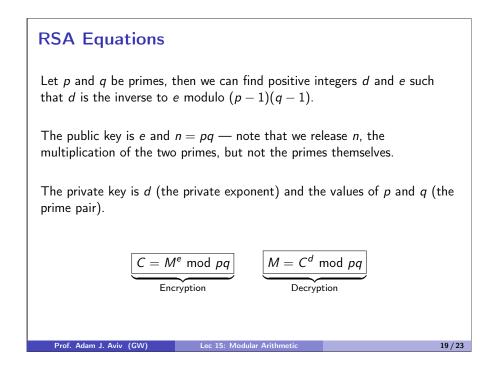






Lec 15: Modular Arithmetic

18 / 23



Example RSA Encryption
Let's label the English alphabet as $A = 1, B = 2, C = 3,, Z = 26$ , and public key is $n = 55$ and $e = 3$ .
We can encrypt the message "HI" by encrypting each letters, "H" = $8 = M_0$ and "I" = $9 = M_1$ .
$C_0 = 8^3 \mod{55} = 256 \mod{55} = 17$
$C_1 = 9^3 \mod n = 729 \mod n = 14$
Prof. Adam J. Aviv (GW) Lec 15: Modular Arithmetic 20 / 23

## Example RSA decryption (1)

To decrypt we need the secret exponent d for p and q. In our example, p = 11 and q = 5, so (p-1)(q-1) = 40. The positive inverse of e = 3 is d = 27 modulo 40.

 $M_0 = C_0^{27} \mod{55} = 17^{27} \mod{55}$ 

This may seem really difficult to compute, but since its under a modulo, we can solve it by taking successive powers.



<section-header><section-header><equation-block><equation-block><equation-block><equation-block><equation-block><equation-block><equation-block>

