



Some Review: Divisors WILLIAM GMARY

- Set of all integers is $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$
- b divides a (or b is a divisor of a) if a = mb for some m
 - denoted b|a
 - any $b \neq 0$ divides 0
- For any a, 1 and a are trivial divisors of a
 - all other divisors of a are called factors of a

4



Primes and Factors

WILLIAM & MARY

- a is prime if it has no non-trivial factors
- examples: 2, 3, 5, 7, 11, 13, 17, 19, 31,...
- Theorem: there are infinitely many primes
- Any integer a > 1 can be factored in a unique way as p₁^a₁ • p₂^a₂ • ... p_t^a_t
 - where all $p_1>p_2>...>p_t$ are prime numbers and where each $a_i>0$

Examples:

91 = 13¹×7¹

11011 = 13¹ ×11² ×7¹

5



Common Divisors

WILLIAM & MARY

 A number d that is a divisor of both a and b is a common divisor of a and b

Example: common divisors of 30 and 24 are 1, 2, 3, 6

• If d|a and d|b, then d|(a+b) and d|(a-b)Example: Since 3 | 30 and 3 | 24, 3 | (30+24) and 3 | (30-24)

If d|a and d|b, then d|(ax+by) for any

integers x and y

Example: $3 \mid 30 \text{ and } 3 \mid 24 \implies 3 \mid (2*30 + 6*24)$

```
Greatest Common Divisor (GCD) WILLIAM gcd(a,b) = max\{k \mid k \mid a \text{ and } k \mid b\}

Example: gcd(60,24) = 12, gcd(a,0) = a

Observations

gcd(a,b) = gcd(|a|, |b|)

gcd(a,b) \leq min(|a|, |b|)

if 0 \leq n, then gcd(an, bn) = n*gcd(a,b)

For all positive integers d, a, and b...

... if d \mid ab

... and gcd(a,d) = 1

... then d \mid b
```

GCD (Cont'd)

GCD (cont'd)

Computing GCD by hand:

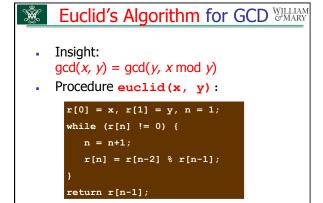
if $a = p_1^{a1} p_2^{a2} \dots p_r^{ar}$ and $b = p_1^{b1} p_2^{b2} \dots p_r^{br}$,

...where $p_1 < p_2 < \dots < p_r$ are prime,

...and a_i and b_i are nonnegative,

...then $gcd(a, b) = p_1^{\min(a1, b1)} p_2^{\min(a2, b2)} \dots p_r^{\min(ar, br)}$ Slow way to find the GCD

requires factoring a and b first (which can be slow)

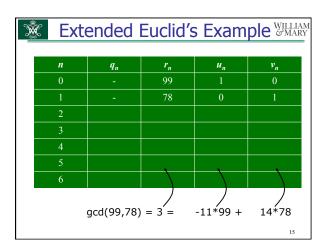


	WILLIAM & MARY	
n	r _n	
0	595	
1	408	
2	595 mod 408 = 187	
3	408 mod 187 = 34	
4	187 mod 34 = 17	
5	34 mod 17 = 0	
gcd(59	5,408) = 17	
		10

Ŵ		Running Time	WILLIAM & MARY
	Runnina	time is logarithmic in size of x and	
		se occurs when ???	
		Enter x and y: 102334155 63245986	
		Step 1: r[i] = 39088169	
		Step 2: $r[i] = 24157817$	
		Step 3: r[i] = 14930352	
		Step 4: $r[i] = 9227465$	
		Step 34: r[i] = 5 Step 35: r[i] = 3 Step 36: r[i] = 2	
		Step $35: r[i] = 3$	
		Step 36: $r[i] = 2$	
		Step 37: $r[i] = 1$	
		Step 38: $r[i] = 0$	
		gcd of 102334155 and 63245986 is	

Let £C(x,y) = {ux+vy: x,y ∈ Z} be the set of linear combinations of x and y Theorem: if x and y are any integers > 0, then gcd(x,y) is the smallest positive element of £C(x,y) Euclid's algorithm can be extended to compute u and v, as well as gcd(x,y) Procedure exteuclid(x, y): (next page...)

×	Exte	ended I	Euclid's	Exam	ple WILLIAM GMARY
	n	q_n	r_n	u_n	v_n
	0	-	595	1	0
	1	-	408	0	1
	2	1	187	1	-1
	3	2	34	-2	3
	4	5	17,	11 —	-16
	5	2	0	-24	35
	gcd(!	595,408) =	: 17 =	11*595 +	-16*408



n	q_n	r _n	u _n	v_n
0	-	99	1	0
1	-	78	0	1
2	1	21	1	-1
3	3	15	-3	4
4	1	6	4	-5
5	2	3	-11	14
6	2	0/	26	-33

W.	Relatively Prime	WILLIA & MAR
_	the name of the same male through the	

- Integers a and b are relatively prime iff gcd(a,b) = 1
 - example: 8 and 15 are relatively prime
- Integers $n_1, n_2, ... n_k$ are pairwise relatively prime if $gcd(n_i, n_j) = 1$ for all $i \neq j$

Ž.		WILLIAM &MARY
	Review of Modular Arithmetic	

~~ ~ ~~
AXX
XXX
00.170

Remainders and Congruence MARY

- For any integer a and any positive integer n, there are two unique integers q and r, such that $0 \le r < n$ and a = qn + r
 - r is the remainder of division by n, written r = a mod n

Example: $12 = 2*5 + 2 \implies 2 = 12 \mod 5$

a and b are congruent modulo n, written $a \equiv b \mod n$, if a mod $n = b \mod n$

Example: $7 \mod 5 = 12 \mod 5 \implies 7 \equiv 12 \mod 5$

10



Negative Numbers

WILLIAM & MARY

- In modular arithmetic,
 ...a negative number a is usually replaced by the congruent number b mod n,
 ...where b is the smallest non-negative number
 - ...such that b = a + m*n

Example: $-3 \equiv 4 \mod 7$

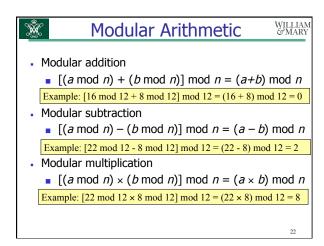
20

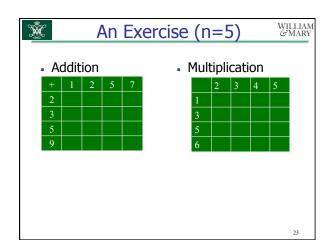


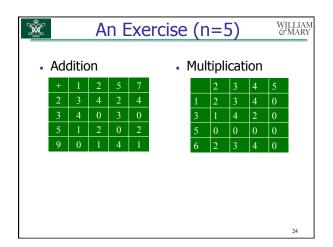
Remainders (Cont'd)

WILLIAM & MARY

- For any positive integer n, the integers can be divided into n equivalence classes according to their remainders modulo n
 - denote the set as Z_n
- i.e., the (mod n) operator maps all integers into the set of integers Z_n={0, 1, 2, ..., (n-1)}







\sim	-2	Serv	^
~	$^{\circ}$	CAN.	-

Properties of Modular Arithmetic WILLIAM SMARY

- Commutative laws
 - $(w + x) \bmod n = (x + w) \bmod n$
 - $(w \times x) \bmod n = (x \times w) \bmod n$
- Associative laws
 - $[(w + x) + y] \mod n = [w + (x + y)] \mod n$
 - $[(w \times x) \times y] \mod n = [w \times (x \times y)] \mod n$
- Distributive law
 - $[w \times (x + y)] \mod n = [(w \times x) + (w \times y)] \mod n$

25



Properties (Cont'd)

WILLIAM & MARY

- Idempotent elements
 - $(0 + m) \bmod n = m \bmod n$
 - $\bullet \quad (1 \times m) \bmod n = m \bmod n$
- Additive inverse (-w)
 - for each $m \in \mathcal{Z}_n$, there exists z such that $(m + z) \mod n = 0$
 - alternatively, $z = (n m) \mod n$

Example: 3 are 4 are additive inverses mod 7, since $(3 + 4) \mod 7 = 0$

- Multiplicative inverse
 - for each positive $m \in \mathcal{Z}_{n'}$ is there a z s.t. $m * z = 1 \mod n$?

26

X

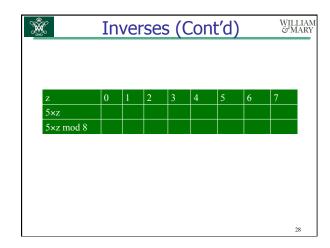
Multiplicative Inverses

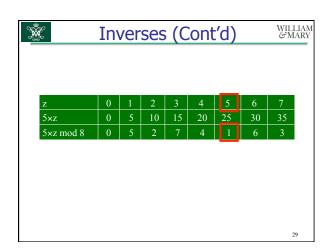
WILLIAM & MARY

- Don't always exist!
 - Ex.: there is no z such that $6 \times z = 1 \mod 8$

z	0	1	2	3	4	5	6	7	
6×z	0	6	12	18	24	30	36	42	
6×z mod 8	0	6	4	2	0	6	4	2	

- An positive integer $m \in \mathbb{Z}_n$ has a multiplicative inverse $m^1 \mod n$ iff $\gcd(m, n) = 1$, i.e., m and n are relatively prime
 - If n is a prime number, then all positive elements in \mathbf{Z}_n have multiplicative inverses



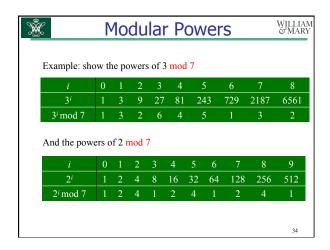


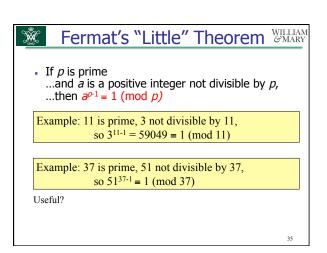
Ŵ	Finding the Multiplicative Inverse	IAM ARY
	Given m and n, how do you find m^1 mod n ?	
-	Extended Euclid's Algorithm exteuclid(m,n): $m^1 \mod n = \mathbf{v}_{n-1}$ if $gcd(m,n) \neq 1$ there is no multiplicative inverse $m^1 \mod n$	
	30	

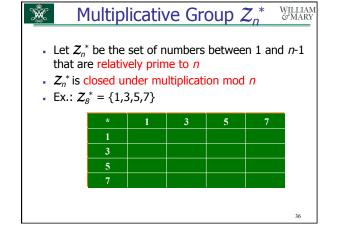
Ŵ	Example WILLIAM & MARK						
	n	q_n	r_n	u _n	v_n		
	0		35	1	0		
	1	-	12	0	1		
	2	2	11	1	-2		
	3	1	1	-1	3		
	4	11	0	12	-35		
gcd(35,12) = 1 = $-1*35 + 3*12$ $12^{-1} \mod 35 = 3$ (i.e., $12*3 \mod 35 = 1$)							
					31		

Ŵ	Modular Division	VILLIAM SMARY
	f the inverse of $b \mod n$ exists, then $a \mod n$ / ($b \mod n$) = ($a * b^1$) mod n)
Е	xample: (13 mod 11) / (4 mod 11) = (13*4 ⁻¹ mod 11) = (13 * 3) mod 11 = 6	
Е	xample: (8 mod 10) / (4 mod 10) not defined since 4 does not have a multiplicative inverse mod 10	

Ŵ		WILLIAM &MARY	
Modular Exponentiation (Power)			







Ŵ

The Totient Function

WILLIAM & MARY

• $\phi(n) = |Z_n^*|$ = the number of integers less than n and relatively prime to n

a) if *n* is prime, then $\phi(n) = n-1$

Example: $\phi(7) = 6$

if $n=p^{\alpha}$, where p is prime and $\alpha>0$, then $\phi(n)=(p\text{-}1)*p^{\alpha-1}$

Example: $\phi(25) = \phi(5^2) = 4*5^1 = 20$

if $n=p^*q$, and p, q are relatively prime, then $\phi(n) = \phi(p)^*\phi(q)$

Example: $\phi(15) = \phi(5*3) = \phi(5) * \phi(3) = 4 * 2 = 8$

27



Euler's Theorem

WILLIAM & MARY

• For every a and n that are relatively prime, $a^{o(n)} \equiv 1 \mod n$

Example: For a = 3, n = 10, which relatively prime: $\phi(10) = 4$ $3^{\phi(10)} = 3^4 = 81 = 1 \mod 10$

Example: For a = 2, n = 11, which are relatively prime: $\phi(11) = 10$ $2^{\phi(11)} = 2^{10} = 1024 = 1 \mod 11$

38



More Euler...

WILLIAM & MARY

• Variant: for all n, $a^{k\phi(n)+1} \equiv a \mod n$ for all a in \mathbb{Z}_n^* , and all nonnegative k

Example: for n = 20, a = 7, $\phi(n) = 8$, and k = 3: $7^{3*8+1} \equiv 7 \mod 20$

Generalized Euler's Theorem: for n = pq (p and q distinct primes), $a^{kq(n)+1} \equiv a \mod n$ for all a in \mathbb{Z}_{pr} and all non-negative k

Example: for n = 15, a = 6, $\phi(n) = 8$, and k = 3: $6^{3*8+1} = 6 \mod 15$



Modular Exponentiation

WILLIAM & MARY

• $x^y \mod n = x^{y \mod \phi(n)} \mod n$

Example: x = 5, y = 7, n = 6, $\phi(6) = 2$

 $5^7 \mod 6 = 5^7 \mod 2 \mod 6 = 5 \mod 6$

• by this, if $y \equiv 1 \mod \phi(n)$, then $x^y \mod n \equiv x \mod$

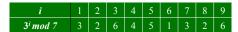
Example:

x = 2, y = 101, n = 33, $\phi(33) = 20$, $101 \mod 20 = 1$ $2^{101} \mod 33 = 2 \mod 33$



The Powers of An Integer, Modulo n

- Consider the expression $a^m \equiv 1 \mod n$
- If a and n are relatively prime, then there is at least one integer *m* that satisfies the above equation
- Ex: for a = 3 and n = 7, what is m?

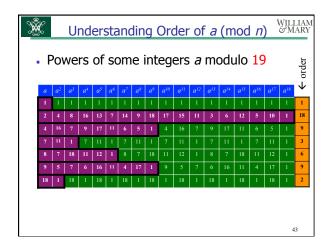




The Power (Cont'd)

WILLIAM & MARY

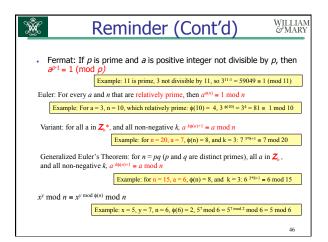
- The least positive exponent *m* for which the above equation holds is referred to
 - the *order of a (mod n),* or
 - the length of the period generated by a





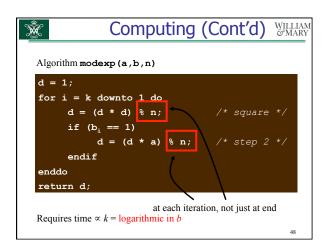
- The length of each period divides 18= $\phi(19)$
 - i.e., the lengths are 1, 2, 3, 6, 9, 18
- Some of the sequences are of length 18
 - e.g., the base $\frac{2}{n}$ generates (via powers) all members of \mathcal{Z}_n^*
 - The base is called the primitive root
 - The base is also called the generator when n is prime

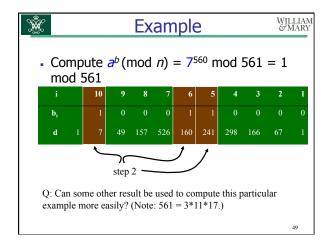
Reminder of Results	WILLIAM & MARY			
Totient function: if n is prime, then $\phi(n) = n-1$ if $n = p^{\alpha}$, where p is prime and $\alpha > 0$, then $\phi(n) = (p-1)*p^{\alpha-1}$ if $n=p^*q$, and p , q are relatively prime, then $\phi(n) = \phi(p)*\phi(q)$				
Example: $\phi(7) = 6$				
Example: $\phi(25) = \phi(5^2) = 4*5^1 = 20$				
Example: $\phi(15) = \phi(5*3) = \phi(5) * \phi(3) = 4 * 2 =$	8			
	45			

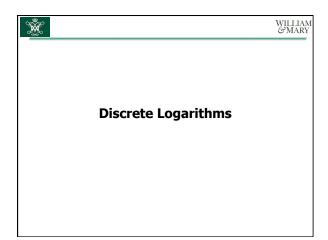




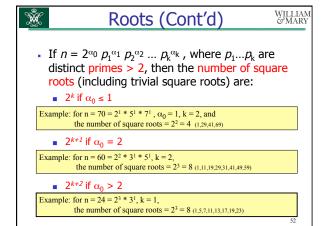
- The repeated squaring algorithm for computing a^b (mod n)
- Let b_i represent the t^h bit of b (total of k bits)







W	Square Roots WILLIAM GMARY		
 x is a non-trivial square root of 1 mod n if it satisfies the equation x² = 1 mod n, but x is neither 1 nor -1 mod n Ex: 6 is a square root of 1 mod 35 since 6² = 1 mod 35 			
 Theorem: if there exists a non-trivial square root of 1 mod n, then n is not a prime 			
	i.e., prime numbers will not have non- trivial square roots		
	51		





Primitive Roots

WILLIAM &MARY

- Reminder: the highest possible order of $a \pmod{n}$ is $\phi(n)$
- If the order of $a \pmod{n}$ is $\phi(n)$, then a is referred to as a *primitive root of n*
 - for a prime number p, if a is a primitive root of p, then a, a^2 , ..., $a^{p\cdot 1}$ are all distinct numbers mod p
- No simple general formula to compute primitive roots modulo n
 - there are methods to locate a primitive root faster than trying out all candidates

53

Ŵ

Primitive Roots (Cont'd)

WILLIAM & MARY

- Theorem: the only integers with primitive roots are of the form 2, 4, p^a, and 2p^a, where
 - *p* is any prime > 2
 - α is a positive integer

Example: for n = 4, $\phi(n) = 2$, primitive roots = $\{3\}$

Example: for $n = 3^2 = 9$, $\phi(n) = 6$, primitive roots = $\{2,5\}$

Example: for n = 19, ϕ (n) = 18, primitive roots = {2,3,10,13,14,15}

Discrete Logarithms WILLIAM WARRY	
 For a primitive root a of a number p, where a^j ≡ b mod p, for some 0 ≤ i ≤ p-1 the exponent i is referred to as the index of b for the base a (mod p), denoted as ind_{a,p}(b) i is also referred to as the discrete logarithm of b to the base a, mod p 	
Logarithms (Cont'd) WILLIAM & MARY	
Example: 2 is a primitive root of 19.	
The powers of 2 mod 19 =	
10 11 12 13 14 15 16 17 18	
17 12 15 5 7 11 4 10 9	
Given a , i , and p , computing $b = a^i \mod p$ is straightforward	
-90	
Computing Discrete Logarithm MARY	
• However, given a , b , and p , computing $\mathbf{i} =$	
ind _{a,p} (b) is difficult ■ Used as the basis of some public key	
cryptosystems	
1	

