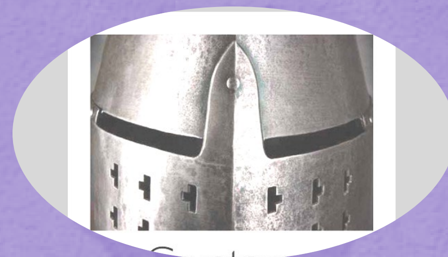


Chapter 2

Introduction to Number Theory

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Divisibility

- We say that a nonzero b **divides** a if $a = mb$ for some m, where a, b, and m are integers
- b divides a if there is no remainder on division
- The notation $b \mid a$ is commonly used to mean b divides a
- If $b \mid a$ we say that b is a **divisor** of a

The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24
$13 \mid 182$; $-5 \mid 30$; $17 \mid 289$; $-3 \mid 33$; $17 \mid 0$

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Properties of Divisibility

- If $a \mid 1$, then $a = \pm 1$
- If $a \mid b$ and $b \mid a$, then $a = \pm b$
- Any $b \neq 0$ divides 0
- If $a \mid b$ and $b \mid c$, then $a \mid c$

$$\boxed{11 \mid 66 \text{ and } 66 \mid 198 = 11 \mid 198}$$

- If $b \mid g$ and $b \mid h$, then $b \mid (mg + nh)$ for arbitrary integers m and n

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Properties of Divisibility

- To see this last point, note that:
  - If $b \mid g$, then g is of the form $g = b * g_1$ for some integer g_1
  - If $b \mid h$, then h is of the form $h = b * h_1$ for some integer h_1
- So:
  - $mg + nh = mbg_1 + nbh_1 = b * (mg_1 + nh_1)$

    and therefore b divides $mg + nh$

$b = 7$; $g = 14$; $h = 63$; $m = 3$; $n = 2$
$7 \mid 14$ and $7 \mid 63$.
To show 7 $(3 * 14 + 2 * 63)$,
we have $(3 * 14 + 2 * 63) = 7(3 * 2 + 2 * 9)$,
and it is obvious that $7 \mid (7(3 * 2 + 2 * 9))$.

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Division Algorithm

- Given any positive integer n and any integer a, if we divide a by n we get an integer quotient q and an integer remainder r that obey the following relationship:

$$a = qn + r \qquad 0 \leq r < n;\ q = \lfloor a/n \rfloor$$

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

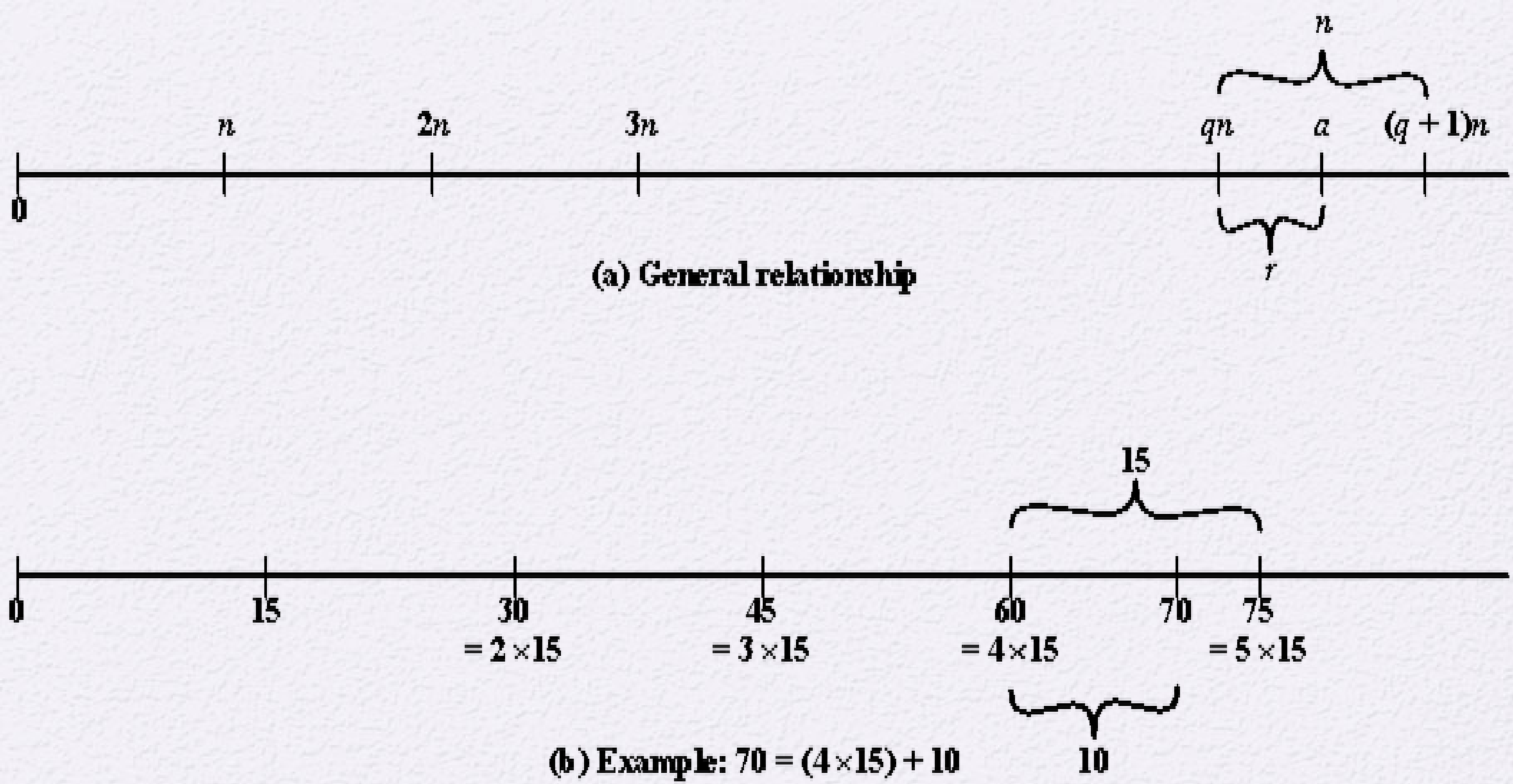


Figure 2.1 The Relationship $a = qn + r;\ 0 \leq r < n$

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Euclidean Algorithm

- One of the basic techniques of number theory
- Procedure for determining the greatest common divisor of two positive integers
- Two integers are **relatively prime** if their only common positive integer factor is 1

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Greatest Common Divisor (GCD)

- The greatest common divisor of *a* and *b* is the largest integer that divides both *a* and *b*
- We can use the notation gcd(*a*,*b*) to mean the **greatest common divisor** of *a* and *b*
- We also define gcd(0,0) = 0
- Positive integer *c* is said to be the gcd of *a* and *b* if:
  - c is a divisor of *a* and *b*
  - Any divisor of *a* and *b* is a divisor of c
- An equivalent definition is:

$$\gcd(a,b) = \max[k, \text{ such that } k \mid a \text{ and } k \mid b]$$

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

GCD

- Because we require that the greatest common divisor be positive, $\gcd(a,b) = \gcd(a,-b) = \gcd(-a,b) = \gcd(-a,-b)$

- In general, $\gcd(a,b) = \gcd(|a|, |b|)$

$$\boxed{\gcd(60, 24) = \gcd(60, -24) = 12}$$

- Also, because all nonzero integers divide 0, we have $\gcd(a,0) = |a|$

- We stated that two integers *a* and *b* are relatively prime if their only common positive integer factor is 1; this is equivalent to saying that *a* and *b* are relatively prime if $\gcd(a,b) = 1$

> 8 and 15 are relatively prime because the positive divisors of 8 are 1, 2, 4, and 8, and the positive divisors of 15 are 1, 3, 5, and 15. So 1 is the only integer on both lists.

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Same GCD

GCD GCD

$$710 = 2 \times 310 + 90$$

$$310 = 3 \times 90 + 40$$

$$90 = 2 \times 40 + 10$$

$$40 = 4 \times 10$$

Figure 2.3 Euclidean Algorithm Example: gcd(710, 310)

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

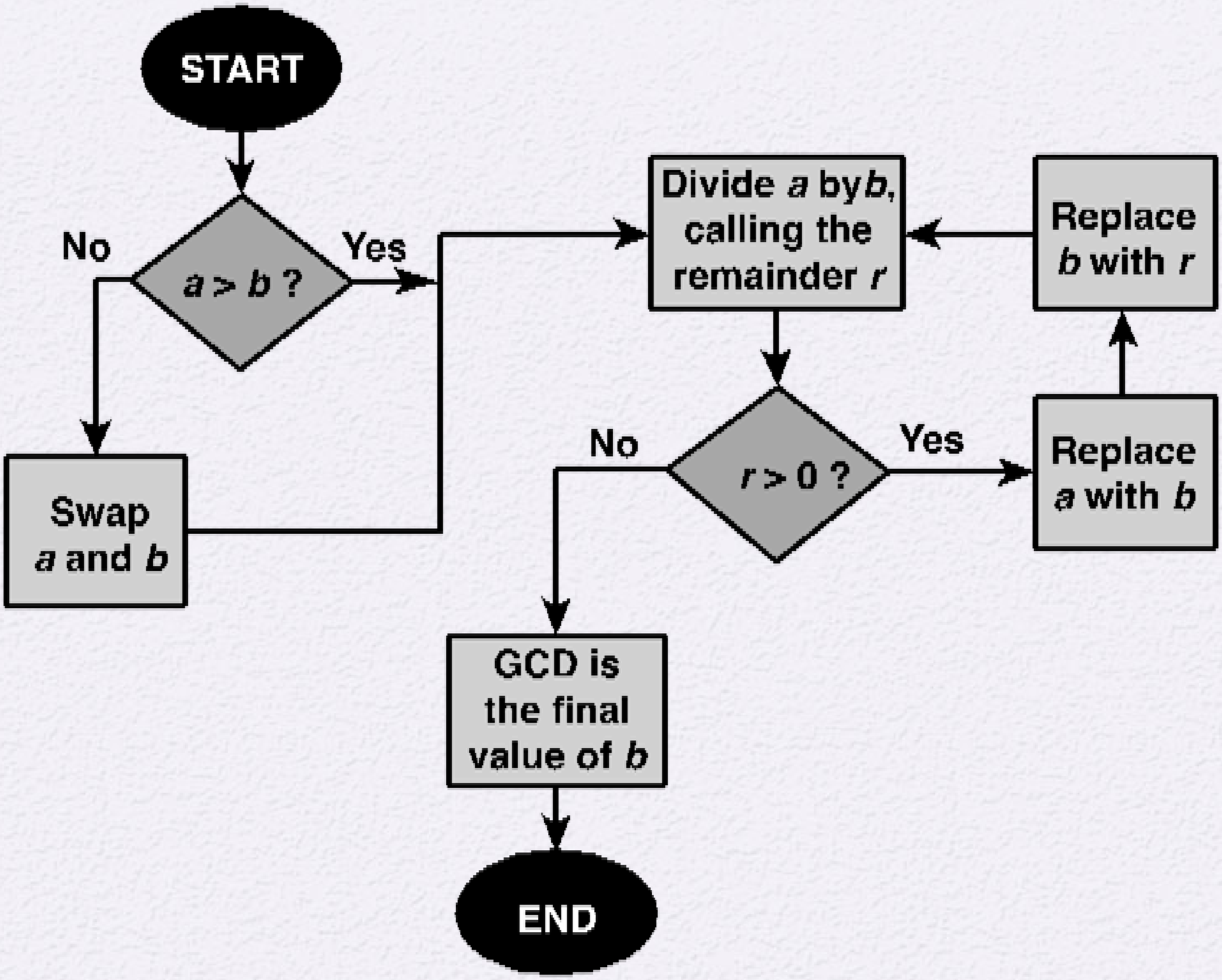


Figure 2.2 Euclidean Algorithm

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Table 2.1
Euclidean Algorithm Example

Dividend	Divisor	Quotient	Remainder
a = 1160718174	b = 316258250	q_1 = 3	r_1 = 211943424
b = 316258250	r_1 = 211943424	q_2 = 1	r_2 = 104314826
r_1 = 211943424	r_2 = 104314826	q_3 = 2	r_3 = 3313772
r_2 = 104314826	r_3 = 3313772	q_4 = 31	r_4 = 1587894
r_3 = 3313772	r_4 = 1587894	q_5 = 2	r_5 = 137984
r_4 = 1587894	r_5 = 137984	q_6 = 11	r_6 = 70070
r_5 = 137984	r_6 = 70070	q_7 = 1	r_7 = 67914
r_6 = 70070	r_7 = 67914	q_8 = 1	r_8 = 2156
r_7 = 67914	r_8 = 2156	q_9 = 31	r_9 = 1078
r_8 = 2156	r_9 = 1078	q_{10} = 2	r_{10} = 0

(This table can be found on page 30 in the textbook)

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Modular Arithmetic

- The modulus
  - If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n; the integer n is called the **modulus**
  - Thus, for any integer a:

$$a = qn + r \qquad 0 \leq r < n; \ q = \lfloor a/n \rfloor$$

$$a = \lfloor a/n \rfloor * n + (a \bmod n)$$

11 mod 7 = 4; - 11 mod 7 = 3

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Modular Arithmetic

- Congruent modulo n
  - Two integers a and b are said to be **congruent modulo *n*** if $(a \bmod n) = (b \bmod n)$
  - This is written as $a \equiv b \pmod{n}$
  - Note that if $a \equiv 0 \pmod{n}$, then $n \mid a$

$73 \equiv 4 \pmod{23}$; $21 \equiv -9 \pmod{10}$

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Properties of Congruences

- Congruences have the following properties:

  1. $a \equiv b \pmod{n}$ if $n \mid (a - b)$

  2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$

  3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$

- To demonstrate the first point, if $n\ (a - b)$, then $(a - b) = kn$ for some k
  - So we can write $a = b + kn$
  - Therefore, (a mod n) = (remainder when $b + kn$ is divided by n) = (remainder when b is divided by n) = (b mod n)

$23 \equiv 8 \pmod{5}$ because $23 - 8 = 15 = 5 * 3$
$-11 \equiv 5 \pmod{8}$ because $-11 - 5 = -16 = 8 * (-2)$
$81 \equiv 0 \pmod{27}$ because $81 - 0 = 81 = 27 * 3$

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Modular Arithmetic

- Modular arithmetic exhibits the following properties:

  1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
  2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
  3. $[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$

- We demonstrate the first property:
  - Define $(a \bmod n) = r_a$ and $(b \bmod n) = r_b$. Then we can write $a = r_a + jn$ for some integer j and $b = r_b + kn$ for some integer k
  - Then:

$$
\begin{aligned}
(a + b) \bmod n &= (ra + jn + rb + kn) \bmod n \\
&= (ra + rb + (k + j)n) \bmod n \\
&= (ra + rb) \bmod n \\
&= [(a \bmod n) + (b \bmod n)] \bmod n
\end{aligned}
$$

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Remaining Properties:

- Examples of the three remaining properties:

11 mod 8 = 3; 15 mod 8 = 7

[(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2

(11 + 15) mod 8 = 26 mod 8 = 2

[(11 mod 8) - (15 mod 8)] mod 8 = - 4 mod 8 = 4

(11 - 15) mod 8 = - 4 mod 8 = 4

[(11 mod 8) * (15 mod 8)] mod 8 = 21 mod 8 = 5

(11 * 15) mod 8 = 165 mod 8 = 5

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Modular Arithmetic Inverses

- Modular Additive Inverse
  - If ***(a + b)mod n = 0***, then ***a*** and ***b*** are modular additive inverses of each other ***mod n.***

- Modular Multiplicative Inverses
  - If ***(a * b)mod n = 1***, then ***a*** and ***b*** are modular multiplicative inverses of each other ***mod n.***

© 2020 Pearson Education, Inc.,
Hoboken, NJ. All rights reserved.

Modular Arithmetic Inverses

- Modular additive inverses can be used to carry out subtraction operations ***mod n***
  - $(a - b) \bmod n = (a + (-b)) \bmod n$, where $-b$ is the modular additive inverse of b.

- Modular multiplicative inverses can be used to carry out division operations ***mod n***
  - $(a / b) \bmod n = (a * (b^{-1})) \bmod n$, where b^{-1} is the modular multiplicative inverse of b.

© 2020 Pearson Education, Inc.,
Hoboken, NJ. All rights reserved.

Table 2.2(a) Arithmetic Modulo 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

(This table can be found on page 33 in the textbook)

Table 2.2(b) Multiplication Modulo 8

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

(This table can be found on page 33 in the textbook)

Table 2.2(c)

Additive and Multiplicative Inverse Modulo 8

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

(This table can be found on page 33 in the textbook)

$$\textbf{if } (a + b) \equiv (a + c) \pmod{n} \textbf{ then } b \equiv c \pmod{n}$$

✘ $$\textbf{if } (a \times b) \equiv (a \times c) \pmod{n} \textbf{ then } b \equiv c \pmod{n}$$

Properties of Modular Arithmetic for Integers in Z_n

Property	Expression
Commutative Laws	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$
Associative Laws	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
Distributive Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
Identities	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
Additive Inverse $(-w)$	For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$

(This table can be found on page 34 in the textbook)

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Extended Euclidean Algorithm

- The extended Euclidean algorithm can be used to calculate the modular multiplicative inverse
  1. Assume ***a > b***
  2. If ***gcd(a,b) =1*** i.e. they are mutually prime
  3. Then the modular multiplicative inverse of ***b mod a = y***; ***y*** derived from solving for ***ax + by = d*** using the extended Euclidean algorithm

- From the previous example the modular multiplicative inverse of ***550 mod 1759*** is ***355*** since ***gcd(1759,550) = 1***

© 2020 Pearson Education, Inc.,
Hoboken, NJ. All rights reserved.

Extended Euclidean Algorithm Example

Used to find ***x*** and ***y*** such that ***ax + by = d = gcd(a,b)***

Extended Euclidean Algorithm			
Calculate	**Which satisfies**	**Calculate**	**Which satisfies**
$r_{-1} = a$		$x_{-1} = 1; y_{-1} = 0$	$a = ax_{-1} + by_{-1}$
$r_0 = b$		$x_0 = 0; y_0 = 1$	$b = ax_0 + by_0$
$r_1 = a \bmod b$ $q_1 = \lfloor a/b \rfloor$	$a = q_1 b + r_1$	$x_1 = x_{-1} - q_1 x_0 = 1$ $y_1 = y_{-1} - q_1 y_0 = -q_1$	$r_1 = ax_1 + by_1$
$r_2 = b \bmod r_1$ $q_2 = \lfloor b/r_1 \rfloor$	$b = q_2 r_1 + r_2$	$x_2 = x_0 - q_2 x_1$ $y_2 = y_0 - q_2 y_1$	$r_2 = ax_2 + by_2$
$r_3 = r_1 \bmod r_2$ $q_3 = \lfloor r_1/r_2 \rfloor$	$r_1 = q_3 r_2 + r_3$	$x_3 = x_1 - q_3 x_2$ $y_3 = y_1 - q_3 y_2$	$r_3 = ax_3 + by_3$
• • •	• • •	• • •	• • •
$r_n = r_{n-2} \bmod r_{n-1}$ $q_n = \lfloor r_{n-2}/r_{n-1} \rfloor$	$r_{n-2} = q_n r_{n-1} + r_n$	$x_n = x_{n-2} - q_n x_{n-1}$ $y_n = y_{n-2} - q_n y_{n-1}$	$r_n = ax_n + by_n$
$r_{n+1} = r_{n-1} \bmod r_n = 0$ $q_{n+1} = \lfloor r_{n-1}/r_n \rfloor$	$r_{n-1} = q_{n+1} r_n + 0$		$d = \gcd(a, b) = r_n$ $x = x_n; y = y_n$

$a = 1759 \quad b = 550$ $\qquad r_i = a x_i + b y_i$

i	$\boxed{r_i = r_{i-2} - r_{i-1} q_i}$	$\boxed{q_i = \frac{r_{i-2}}{r_{i-1}}}$	$\boxed{x_i = x_{i-2} - q_i x_{i-1}}$	$\boxed{y_i = y_{i-2} - q_i y_{i-1}}$
-1	$r_{i-2} = a = 1759$	$-$	1	0
0	$r_{i-1} = b = 550$	$-$	0	1
1	$r_1 = 109$	$q_1 = \lfloor \frac{1759}{550} \rfloor = 3$	$x_1 = 1 - 3(0) = 1$	$y_1 = 0 - 1(3) = -3$
2	$r_2 = 5$	$q_2 = \lfloor \frac{550}{109} \rfloor = 5$	$x_2 = 0 - 1(5) = -5$	$y_2 = 1 - (-3)(5) = 16$
3	$r_3 = 4$	$q_3 = \lfloor \frac{109}{5} \rfloor = 21$	$x_3 = 1 - (-5)(21) = 106$	$y_3 = -3 - 16(21) = -339$
$*4$	$r_4 = 1$	$q_4 = \lfloor \frac{5}{4} \rfloor = 1$	$x_4 = -5 - (106)(1) = \boxed{-111}$	$y_4 = 16 - (-339)(1) = \boxed{355}$
5	$r_5 = 0$	$q_5 = \lfloor \frac{4}{1} \rfloor = 4$		

$= 1$

$$d = \gcd(1759, 550) = \underbrace{1} = ax + by = (1759)(-111) + 550(355)$$

$a(x) \overset{b}{\equiv} 1 \qquad b(y) \overset{a}{\equiv} 1$

$x = a^{-1} \pmod b \qquad y = b^{-1} \bmod a \qquad ax + by = d$

Extended Euclidean Algorithm Example

Used to find ***x*** and ***y*** such that ***ax + by = d = gcd(a,b)***

i	r_i	q_i	x_i	Y_i
–1	1759		1	0
0	550		0	1
1	109	3	1	–3
2	5	5	–5	16
3	4	21	106	–339
4	1	1	–111	355
5	0	4		

Result: d = 1; x = –111; y = 355

(This table can be found on page 39 in the textbook)

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Prime Numbers

- Prime numbers only have divisors of 1 and itself
  - They cannot be written as a product of other numbers
- Prime numbers are central to number theory
- Any integer a > 1 can be factored in a unique way as

$$a = p_1^{a1} * p_2^{a2} * \ldots * p_t^{at}$$

where $p_1 < p_2 < \ldots < p_t$ are prime numbers and where each a_i is a positive integer

- This is known as the fundamental theorem of arithmetic

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Table 2.5
Primes Under 2000

2	101	211	307	401	503	601	701	809	907	1009	1103	1201	1301	1409	1511	1601	1709	1801	1901
3	103	223	311	409	509	607	709	811	911	1013	1109	1213	1303	1423	1523	1607	1721	1811	1907
5	107	227	313	419	521	613	719	821	919	1019	1117	1217	1307	1427	1531	1609	1723	1823	1913
7	109	229	317	421	523	617	727	823	929	1021	1123	1223	1319	1429	1543	1613	1733	1831	1931
11	113	233	331	431	541	619	733	827	937	1031	1129	1229	1321	1433	1549	1619	1741	1847	1933
13	127	239	337	433	547	631	739	829	941	1033	1151	1231	1327	1439	1553	1621	1747	1861	1949
17	131	241	347	439	557	641	743	839	947	1039	1153	1237	1361	1447	1559	1627	1753	1867	1951
19	137	251	349	443	563	643	751	853	953	1049	1163	1249	1367	1451	1567	1637	1759	1871	1973
23	139	257	353	449	569	647	757	857	967	1051	1171	1259	1373	1453	1571	1657	1777	1873	1979
29	149	263	359	457	571	653	761	859	971	1061	1181	1277	1381	1459	1579	1663	1783	1877	1987
31	151	269	367	461	577	659	769	863	977	1063	1187	1279	1399	1471	1583	1667	1787	1879	1993
37	157	271	373	463	587	661	773	877	983	1069	1193	1283		1481	1597	1669	1789	1889	1997
41	163	277	379	467	593	673	787	881	991	1087		1289		1483		1693			1999
43	167	281	383	479	599	677	797	883	997	1091		1291		1487		1697			
47	173	283	389	487		683		887		1093		1297		1489		1699			
53	179	293	397	491		691				1097				1493					
59	181			499										1499					
61	191																		
67	193																		
71	197																		
73	199																		
79																			
83																			
89																			
97																			

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

(This table can be found on page 40 in the textbook)

Fermat's Theorem

- How to solve modulus operation for big numbers?

$$7^{180} = ?\ (\text{mod } 19)$$

Fermat's Theorem

- States the following:
  - If *p* is prime and *a* is a positive integer not divisible by *p* then

$$a^{p-1} \equiv 1 \pmod{p}$$

- An alternate form is:
  - If *p* is prime and *a* is a positive integer, then

$$a^{p} \equiv a \pmod{p}$$

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Fermat's Theorem Examples

$$
\begin{aligned}
&a = 7, p = 19\\
&7^2 = 49 \equiv 11 \pmod{19}\\
&7^4 \equiv 121 \equiv 7 \pmod{19}\\
&7^8 \equiv 49 \equiv 11 \pmod{19}\\
&7^{16} \equiv 121 \equiv 7 \pmod{19}\\
&a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}
\end{aligned}
$$

$$
\begin{array}{ll}
p = 5, a = 3 & a^p = 3^5 = 243 \equiv 3(\bmod 5) = a(\bmod p)\\
p = 5, a = 10 & a^p = 10^5 = 100000 \equiv 10(\bmod 5) \equiv 0(\bmod 5) = a(\bmod p)
\end{array}
$$

Fermat's Theorem

- How to solve modulus operation for big numbers?
  - 7^{180}=? (mod 19)

$$7^{180} = \left(7^{18}\right)^{10} = (1)^{10} = 1(\text{mod } 19)$$

Euler's Totient Function ø(*n*)

- *ø(n)= The number of positive integers less than n and relatively prime to n.*
- $ø(1) = 1$
- $ø(p) = p - 1$ (where p and q are prime)
- $ø(pq) = ø(p)ø(q) = (p-1)(q-1)$

Table 2.6

Some Values of Euler's Totient Function $\phi(n)$

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4

n	$\phi(n)$
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

n	$\phi(n)$
21	12
22	10
23	22
24	8
25	20
26	12
27	18
28	12
29	28
30	8

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

(This table can be found on page 44 in the textbook)

Euler's Theorem

- States that for every *a* and *n* that are relatively prime:

$$a^{\varnothing(n)} \equiv 1 (\text{mod } n)$$

- An alternative form is:

$$a^{\varnothing(n)+1} \equiv a (\text{mod } n)$$

Note: The second form does not require a and n to be relatively prime.

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Euler's Theorem Examples

$$a = 3; n = 10; \phi(10) = 4; \quad a^{\phi(n)} = 3^4 = 81 \equiv 1(\text{mod } 10) \equiv 1(\text{mod } n)$$

$$a = 2; n = 11; \phi(11) = 10; \quad a^{\phi(n)} = 2^{10} = 1024 \equiv 1(\text{mod } 11) \equiv 1(\text{mod } n)$$

Miller-Rabin Algorithm

Miller-Rabin Algorithm

- Typically used to test a large number for primality
- Algorithm is:

TEST (n)

1. - Find integers k, q, with $k > 0$, q odd, so that $(n - 1)=2^k q$;
2. - Select a random integer a, $1 < a < n - 1$;
3. - **if** $a^q \bmod n = 1$ **then** return ("inconclusive") ;
4. - **for** $j = 0$ **to** $k - 1$ **do**
5. - **if** $(a^{2^{\wedge}\{j\}q} \bmod n = n - 1)$ **then** return ("inconclusive") ;
6. - return ("composite") ;

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Miller-Rabin Algorithm

- The pseudocode below can be used to calculate k and q in the first step of the Miller-Rabin Algorithm
- Algorithm is:

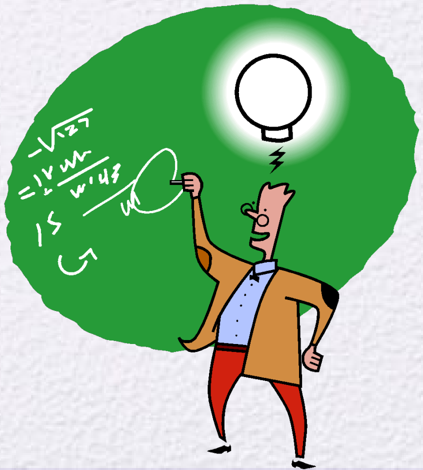
Input (*n*)

1. • $k \leftarrow 0$;
2. • $q \leftarrow (n-1)$;
3. • while ((q mod 2) ==0) /*While q is even*/
4. • { $k \leftarrow k+1$;
5. • $q \leftarrow q/2$; }
6. • return (k,q) ;

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Deterministic Primality Algorithm

- Prior to 2002 there was no known method of efficiently proving the primality of very large numbers
- All of the algorithms in use produced a probabilistic result
- In 2002 Agrawal, Kayal, and Saxena developed an algorithm that efficiently determines whether a given large number is prime
  - Known as the **AKS algorithm**
  - Does not appear to be as efficient as the Miller-Rabin algorithm



© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Chinese Remainder Theorem (CRT)

- Believed to have been discovered by the Chinese mathematician Sun-Tsu in around 100 A.D.
- One of the most useful results of number theory
- Says it is possible to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli
- Can be stated in several ways

Provides a way to manipulate (potentially very large) numbers mod *M* in terms of tuples of smaller numbers

- This can be useful when *M* is 150 digits or more
- However, it is necessary to know beforehand the factorization of *M*

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Chinese Remainder Theorem

- Given pairwise coprime positive integers $n_1, n_2, \cdots, n_k$ and arbitrary integers $a_1, a_2, \cdots, a_k$ the system of equations

$$x \equiv a_1 \ (mod\ n_1)$$

$$x \equiv a_2 \ (mod\ n_2)$$

$$x \equiv a_k \ (mod\ n_k)$$

has a unique solution for x.

Chinese Remainder Theorem

- Algorithm to find a solution for x using the CRT:

1. Compute $N = n_1 \times n_2 \times \cdots \times n_k$.
2. For each $i = 1, 2, \ldots, k$, compute

$$y_i = \frac{N}{n_i} = n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_k.$$

3. For each $i = 1, 2, \ldots, k$, compute $z_i \equiv y_i^{-1} \bmod n_i$ using Euclid's extended algorithm (z_i exists since $n_1, n_2, \ldots, n_k$ are pairwise coprime).
4. The integer $x = \sum_{i=1}^{k} a_i y_i z_i$ is a solution to the system of congruences, and $x \bmod N$ is the unique solution modulo N.

$$x \equiv \overset{a_i}{1} \mod \overset{n_i}{3} \qquad x = ?$$

$$x \equiv 4 \mod 5$$

$$x \equiv 6 \mod 7$$

$$N = n_1 \times n_2 \times n_3 = 3 \cdot 5 \cdot 7 = 105 \qquad Z_i \overset{n_i}{\equiv} y_i^{-1}$$

$$y_i = \frac{N}{n_i} \quad : y_1 = \frac{105}{3} = 35 \longrightarrow 35 Z_1 \overset{3}{\equiv} 1 \longrightarrow 2 Z_1 \overset{3}{\equiv} 1 \longrightarrow Z_1 = 2$$

$$y_2 = \frac{105}{5} = 21 \longrightarrow 21 Z_2 \overset{5}{\equiv} 1 \longrightarrow Z_2 \overset{5}{\equiv} 1 \longrightarrow Z_2 = 1$$

$$y_3 = \frac{105}{7} = 15 \longrightarrow 15 Z_3 \overset{7}{\equiv} 1 \longrightarrow Z_3 \overset{7}{\equiv} 1 \longrightarrow Z_3 = 1$$

$$X = \sum_{i=1}^{3} a_i y_i Z_i = (1)(35)(2) + (4)(21)(1) + (6)(15)(1) =$$

$$70 + 84 + 90 = 244 = 34 \pmod{105}$$

Table 2.7

Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

- The possible primitive roots of prime number 19 are 2, 3, 10, 13, 14 and 15

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

(This table can be found on page 53 in the textbook)

Discrete Logarithms

- Let a be a primitive root of prime number p then for any integer b, we have

$$b \equiv a^i \ (mod\ p) \ where\ 0 \leq i \leq p-1$$

- This exponent i is referred to as the discrete logarithm of b for the base a(mod p).
- We denote this value as $dlog_{a,p}(b)$.

Discrete Logarithms

- The discrete logarithm (***dlog***) ***i*** for an integer ***b*** to the base ***(a,p)*** is written as follows $\mathbf{dlog}_{a,p}\, b = i$
- This implies that $a^i \bmod p = b$
- The integer ***p*** is a prime number and ***a*** is a primitive root of ***p***
- Choosing ***a*** to be a primitive root of ***p*** ensures that a discrete logarithm value exists for values of ***b***
- Discrete Logarithms are used in several cryptographic algorithms

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

Table 2.8

Tables of Discrete Logarithms, Modulo 19

(a) Discrete logarithms to the base 2, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{2,19}(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(b) Discrete logarithms to the base 3, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{3,19}(a)$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

(c) Discrete logarithms to the base 10, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{10,19}(a)$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9

(d) Discrete logarithms to the base 13, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{13,19}(a)$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9

(e) Discrete logarithms to the base 14, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{14,19}(a)$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	4	9

(f) Discrete logarithms to the base 15, modulo 19

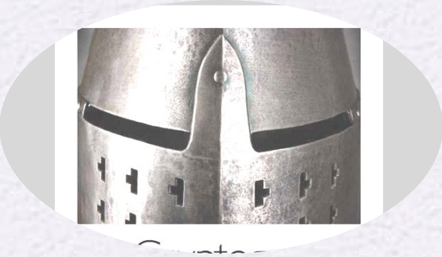
a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{15,19}(a)$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.

(This table can be found on page 56 in the textbook)

Summary

- Understand the concept of divisibility and the division algorithm
- Understand how to use the Euclidean algorithm to find the greatest common divisor
- Present an overview of the concepts of modular arithmetic
- Explain the operation of the extended Euclidean algorithm
- Discuss key concepts relating to prime numbers



- Understand Fermat's theorem
- Understand Euler's theorem
- Define Euler's totient function
- Make a presentation on the topic of testing for primality
- Explain the Chinese remainder theorem
- Define discrete logarithms

© 2020 Pearson Education, Inc., Hoboken, NJ. All rights reserved.