CH.4 Number Theory and Cryptography

4.1 Divisibility and Modular Arithmetic

4.3 Primes and Greatest Common Divisors

Lecture 7

Dr. *Mohamed Abdel-Aal*
Discrete Mathematics

DEFINITION

If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. When a divides b we say that a is a *factor* or *divisor* of b, and that b is a *multiple* of a. The notation $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b.

77 | 7: false bigger number can't divide smaller positive number
7 | 77: true because 77 = 7 · 11
24 | 24: true because 24 = 24 · 1
1 | 2: true, 1 divides everything.
2 | 1: false.
0 | 24: false, only 0 is divisible by 0
24 | 0: true, 0 is divisible by every number (0 = 24 · 0)

Lecture 7

THEOREM

Let a, b, and c be integers, where $a \neq 0$. Then

(i) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;
(ii) if $a \mid b$, then $a \mid bc$ for all integers c;
(iii) if $a \mid b$ and $b \mid c$, then $a \mid c$.

Example:

1. $17|34 \wedge 17|170 \rightarrow 17|204$
2. $17|34 \rightarrow 17|340$
3. $6|12 \wedge 12|144 \rightarrow 6 \mid 144$

COROLLARY

If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

The Division Algorithm

When an integer is divided by a positive integer, there is a quotient and a remainder, as the division algorithm shows.

THE DIVISION ALGORITHM Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

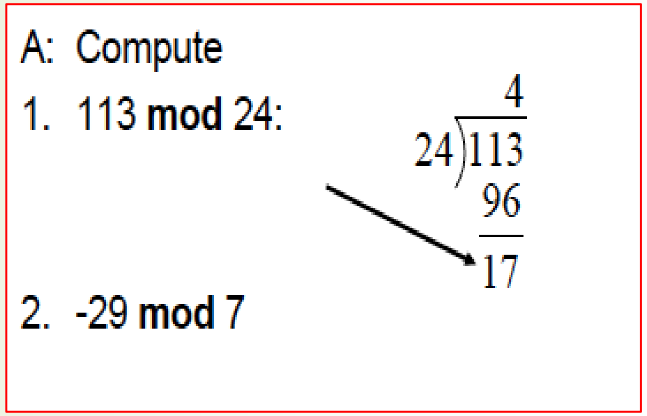
DEFINITION

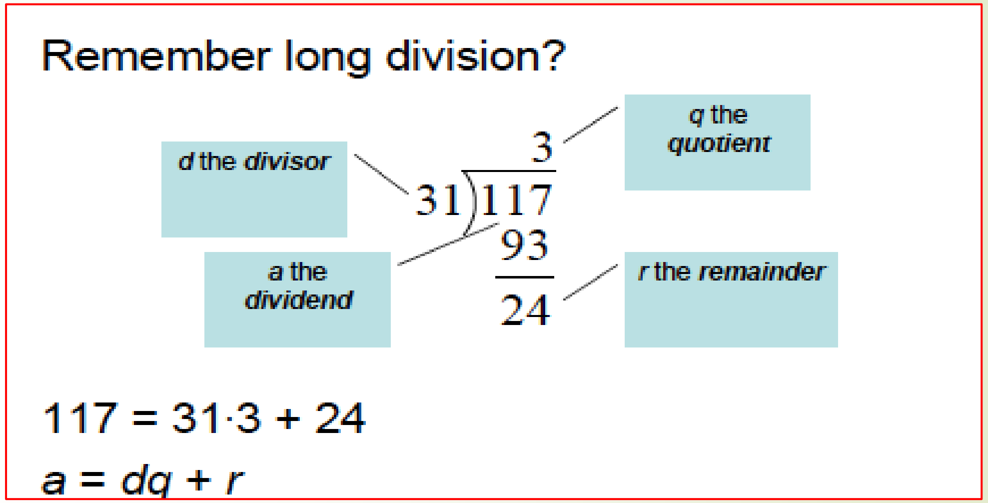
Lecture 7

In the equality given in the division algorithm, d is called the *divisor*, a is called the *dividend*, q is called the *quotient*, and r is called the *remainder*. This notation is used to express the quotient and remainder:

$$q = a \textbf{ div } d, \quad r = a \textbf{ mod } d.$$

Remark: ***Note that both a div d and a mod d for a fixed d are functions on the set of integers.*** Furthermore, when a is an integer and d is a positive integer, we have a **div d =** $\lfloor$**a/d**$\rfloor$ and a **mod d = a - d.**





Example

What are the quotient and remainder when 101 is divided by 11?

We have

Hence, the quotient when 101 is divided by 11 is 9 = **101 div 11**, and the remainder is 2 = **101 mod 11**.

Example

What are the quotient and remainder when -11 is divided by 3?

$$-11 = 3(-3) - 2,$$

Note that the remainder cannot be negative. Consequently, the remainder is *not -2, even* though

$$-11 = 3(-3) - 2,$$

because r = -2 does not satisfy $0 \le r < 3$.

We have $-11 = 3(-4) + 1.$

Hence, the quotient when -11 is divided by 3 is -4 = **-11 div 3, and the remainder is** 1 = **-11 mod 3.**

Note that the integer a is divisible by the integer d if and only if the remainder is zero when a is divided by d.

Modular Arithmetic

DEFINITION 3 If a and b are integers and m is a positive integer, then a is *congruent to b modulo m* if m divides $a - b$. We use the notation $a \equiv b \pmod{m}$ to indicate that a is congruent to b modulo m. We say that $a \equiv b \pmod{m}$ is a **congruence** and that m is its **modulus** (plural **moduli**). If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$.

Although both notations **a ≡ b (mod m)** and **a mod m = b** include "mod," they represent fundamentally different concepts. The first represents a relation on the set of integers, whereas the second represents a function. However, the relation a ≡ b (mod m) and the **mod** m function are closely related, as described in Theorem 3.

Lecture 7

THEOREM 3 Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Recall that a **mod** m and b **mod** m are the remainders when a and b are divided by m, respectively. Consequently, Theorem 3 also says that **a $\equiv$ b (mod m)** if and only if **a and b have the same remainder** when divided by m.

Example

Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution

Because 6 divides $17 - 5 = 12$, we see that $17 \equiv 5 \pmod 6$. However, because $24 - 14 = 10$ is not divisible by 6, we see that $24 \not\equiv 14 \pmod 6$

THEOREM 4 Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Example

Find a **div** m and a **mod** m when

a) $a = 228$, $m = 119$.

b) $a = 9009$, $m = 223$.

c) $a = -10101$, $m = 333$.

Solution

Recall that a div m and a **mod** m are the integer quotient and remainder when a is divided by m.

a) Because $228 = 1 \cdot 119 + 109$, we have 228 div 119 = 1 and 228 **mod** 119 = 109.

b) Because $9009 = 40 \cdot 223 + 89$, we have 9009 div 223 = 40 and 9009 **mod** 223 = 89.

c) Because $-10101 = -31 \cdot 333 + 222$, we have -10101 div 333 = -31 and -10101 **mod** 333 = 222. (Note that 10101 ÷ 333 is $30\,\frac{111}{333}$, so without the negative dividend we would get a different absolute quotient and different remainder. But we have to round the negative quotient here, $-30\,\frac{111}{333}$, down to -31 in order for the remainder to be nonnegative.)

Lecture 7

Theorem 5 shows that additions and multiplications preserve congruences.

THEOREM 5 Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac \equiv bd \pmod{m}.$$

Because $7 = 2 \pmod{5}$ and $11 = 1 \pmod{5}$, it follows from Theorem 5 that
$18 = 7 + 11 = 2 + 1 = 3 \pmod{5}$

and that $77 = 7 \cdot 11 = 2 \cdot 1 = 2 \pmod{5}$.

COROLLARY 2 Let m be a positive integer and let a and b be integers. Then

$$(a + b) \textbf{ mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m)) \textbf{ mod } m$$

and

$$ab \textbf{ mod } m = ((a \textbf{ mod } m)(b \textbf{ mod } m)) \textbf{ mod } m.$$

Lecture 7

Arithmetic Modulo m

We can define arithmetic operations on Z_m, the set of nonnegative integers less than m, that is, the set $\{0, 1,\ldots,m-1\}$. In particular, we define addition of these integers, denoted by $+_m$ by

$$a +_m b = (a + b) \ \mathbf{mod\ m},$$

we define multiplication of these integers, denoted by $\cdot_m$ by

$$a \cdot_m b = (a \cdot b) \ \mathbf{mod\ m},$$

Example

Use the definition of addition and multiplication in Z_m to find $7 +_{11} 9$ and $7 \cdot_m 9$.

Solution

Using the definition of addition modulo 11, we find that

$7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5,$

And

$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8.$

Hence $7 +_{11} 9 = 5$ and $7 \cdot_{11} 9 = 8$.

Quis

Find a **div** m and a **mod** m when

a) $a = 228$, $m = 119$.
b) $a = 9009$, $m = 223$.
c) $a = -10101$, $m = 333$.
d) $a = -765432$, $m = 38271$.

Find the integer a such that

a) $a \equiv 43 \pmod{23}$ and $-22 \le a \le 0$.
b) $a \equiv 17 \pmod{29}$ and $-14 \le a \le 14$.
c) $a \equiv -11 \pmod{21}$ and $90 \le a \le 110$.

Find the integer a such that

a) $a \equiv -15 \pmod{27}$ and $-26 \le a \le 0$.
b) $a \equiv 24 \pmod{31}$ and $-15 \le a \le 15$.
c) $a \equiv 99 \pmod{41}$ and $100 \le a \le 140$.

Find each of these values.

a) $(-133 \textbf{ mod } 23 + 261 \textbf{ mod } 23) \textbf{ mod } 23$
b) $(457 \textbf{ mod } 23 \cdot 182 \textbf{ mod } 23) \textbf{ mod } 23$

Find each of these values.

a) $(99^2 \textbf{ mod } 32)^3 \textbf{ mod } 15$
b) $(3^4 \textbf{ mod } 17)^2 \textbf{ mod } 11$
c) $(19^3 \textbf{ mod } 23)^2 \textbf{ mod } 31$
d) $(89^3 \textbf{ mod } 79)^4 \textbf{ mod } 26$

Lecture 7

Primes and Greatest Common Divisors

Primes

DEFINITION 1	An integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite*.

***Remark*: The integer n is composite if and only if there exists an integer a such that $a \mid n$ and** $1 < a < n$.

Example

- The integer 7 is prime because its only positive factors are 1 and 7, whereas the integer 9 is composite because it is divisible by 3.

Lecture 7

THEOREM 1 **THE FUNDAMENTAL THEOREM OF ARITHMETIC** Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

- The prime factorizations of 100, 641, 999, and 1024 are given by

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2,$$
$$641 = 641,$$
$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37,$$
$$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}.$$

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Lecture 7

Example

Show that 101 is prime.

Solution

The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer), it follows that 101 is prime.

Greatest Common Divisors and Least Common Multiples

DEFINITION 2

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

Example

What is the greatest common divisor of 24 and 36?

Solution

The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12. Hence, gcd(24, 36) = 12.

Lecture 7

Example

What is the greatest common divisor of 17 and 22?

The integers 17 and 22 have no positive common divisors other than 1, so that gcd(17, 22) = 1.

DEFINITION 3 The integers a and b are *relatively prime* if their greatest common divisor is 1.

- the integers 17 and 22 are relatively prime, because gcd(17, 22) = 1

DEFINITION 4 The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

Example

- Determine whether the integers 10, 17, and 21 are pairwise relatively prime and whether the integers 10, 19, and 24 are pairwise relatively prime.

Because gcd(10, 17) = 1, gcd(10, 21) = 1, and gcd(17, 21) = 1, we conclude that 10, 17, and 21 are pairwise relatively prime.
Because gcd(10, 24) = 2 > 1, we see that 10, 19, and 24 are not pairwise relatively prime.

DEFINITION 5 The *least common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $\operatorname{lcm}(a, b)$.

Another way to find the greatest common divisor of two positive integers is to use the prime factorizations of these integers. Suppose that the prime factorizations of the positive integers a and b are

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \; b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n},$$

where each exponent is a nonnegative integer, and where all primes occurring in the prime factorization of either a or b are included in both factorizations, with zero exponents if necessary. Then $\gcd(a, b)$ is given by

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)},$$

$$\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)},$$

Lecture 7

Example

Because the prime factorizations of 120 and 500 are $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, the greatest common divisor is

$$\gcd(120, 500) = 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)} = 2^2 3^0 5^1 = 20.$$

Example

What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

$$\operatorname{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^4 3^5 7^2.$$

Lecture 7

THEOREM 5 Let a and b be positive integers. Then

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b).$$

The Euclidean Algorithm

LEMMA 1 Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

Example

Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Solution

Successive uses of the division algorithm give:

$$662 = 414 \cdot 1 + 248$$
$$414 = 248 \cdot 1 + 166$$
$$248 = 166 \cdot 1 + 82$$
$$166 = 82 \cdot 2 + 2$$
$$82 = 2 \cdot 41.$$

Hence, $\gcd(414, 662) = 2$, because 2 is the last nonzero remainder.

gcds as Linear Combinations

THEOREM 6 **BÉZOUT'S THEOREM** If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.

Example

Express gcd(252, 198) = 18 as a linear combination of 252 and 198.

Solution

To show that gcd(252, 198) = 18, the Euclidean algorithm uses these divisions:

$$252 = 1 \cdot 198 + 54$$
$$198 = 3 \cdot 54 + 36$$
$$54 = 1 \cdot 36 + 18$$
$$36 = 2 \cdot 18$$

Using the next-to-last division (the third division), we can express gcd(252, 198) = 18 as a linear combination of 54 and 36. We find that: $18 = 54 - 1 \cdot 36$.

The second division tells us that

$36 = 198 - 3 \cdot 54$.

Substituting this expression for 36 into the previous equation, we can express 18 as a linear combination of 54 and 198. We have

$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198.$

The first division tells us that

$54 = 252 - 1 \cdot 198.$

Substituting this expression for 54 into the previous equation, we can express 18 as a linear combination of 252 and 198. We conclude that

$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198,$

completing the solution.

Example

Express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

Solution

a) 10, 11 b) 21, 44 c) 36, 48

a) This first one is easy to do by inspection. Clearly 10 and 11 are relatively prime, so their greatest common divisor is 1, and $1 = 11 - 10 = (-1) \cdot 10 + 1 \cdot 11$.

Lecture 7

b) In order to find the coefficients s and t such that $21s + 44t = \gcd(21, 44)$, we carry out the steps of the Euclidean algorithm.

$$44 = 2 \cdot 21 + 2$$

$$21 = 10 \cdot 2 + 1$$

Then we work up from the bottom, expressing the greatest common divisor (which we have just seen to be 1) in terms of the numbers involved in the algorithm, namely 44, 21, and 2. In particular, the last equation tells us that $1 = 21 - 10 \cdot 2$, so that we have expressed the gcd as a linear combination of 21 and 2. But now the first equation tells us that $2 = 44 - 2 \cdot 21$; we plug this into our previous equation and obtain

$$1 = 21 - 10 \cdot (44 - 2 \cdot 21) = 21 \cdot 21 - 10 \cdot 44 .$$

Thus we have expressed 1 as a linear combination (with integer coefficients) of 21 and 44, namely $\gcd(21, 44) = 21 \cdot 21 + (-10) \cdot 44$.

Use the Euclidean algorithm to find

a) $\gcd(1, 5)$.
b) $\gcd(100, 101)$.
c) $\gcd(123, 277)$.
d) $\gcd(1529, 14039)$.

Lecture 7

Q: Compute the following.

1. 307^{1001} **mod** 102
2. $(-45 \cdot 77)$ **mod** 17

A: Use the previous identities to help simplify:

1. Using multiplication rules, before multiplying (or exponentiating) can reduce modulo 102:

307^{1001} **mod** $102 \equiv 307^{1001} \pmod{102}$

$\equiv 1^{1001} \pmod{102} \equiv 1 \pmod{102}$. Therefore, 307^{1001} **mod** 102 = 1.

A: Use the previous identities to help simplify:

2. Repeatedly reduce after each multiplication:

$(-45 \cdot 77)$ **mod** $17 \equiv (-45 \cdot 77) \pmod{17}$

$\equiv (6 \cdot 9) \pmod{17} \equiv 54 \pmod{17} \equiv 3 \pmod{17}$. Therefore $(-45 \cdot 77)$ **mod** 17 = 3.

Lecture 7

1. Determine whether each of these integers is prime.

a) 21 **b)** 29
c) 71 **d)** 97
e) 111 **f)** 143

In each case we can just use trial division up to the square root of the number being tested.

a) Since $21 = 3 \cdot 7$, we know that 21 is not prime.

b) Since $2 \nmid 29$, $3 \nmid 29$, and $5 \nmid 29$, we know that 29 is prime. We needed to check for prime divisors only up to $\sqrt{29}$, which is less than 6.

c) Since $2 \nmid 71$, $3 \nmid 71$, $5 \nmid 71$, and $7 \nmid 71$, we know that 71 is prime.

d) Since $2 \nmid 97$, $3 \nmid 97$, $5 \nmid 97$, and $7 \nmid 97$, we know that 97 is prime.

e) Since $111 = 3 \cdot 37$, we know that 111 is not prime.

f) Since $143 = 11 \cdot 13$, we know that 143 is not prime.

Lecture 7

33. Use the Euclidean algorithm to find

a) $\gcd(12, 18)$.
b) $\gcd(111, 201)$.
c) $\gcd(1001, 1331)$.
d) $\gcd(12345, 54321)$.
e) $\gcd(1000, 5040)$.
f) $\gcd(9888, 6060)$.

a) By Lemma 1, $\gcd(12,18)$ is the same as the gcd of the smaller of these two numbers (12) and the remainder when the larger (18) is divided by the smaller. In this case the remainder is 6, so $\gcd(12,18) = \gcd(12,6)$. Now $\gcd(12,6)$ is the same as the gcd of the smaller of *these* two numbers (6) and the remainder when the larger (12) is divided by the smaller, namely 0. This gives $\gcd(12,6) = \gcd(6,0)$. But $\gcd(x,0) = x$ for all positive integers, so $\gcd(6,0) = 6$. Thus the answer is 6. In brief (the form we will use for the remaining parts), $\gcd(12,18) = \gcd(12,6) = \gcd(6,0) = 6$.

b) $\gcd(111,201) = \gcd(111,90) = \gcd(90,21) = \gcd(21,6) = \gcd(6,3) = \gcd(3,0) = 3$

c) $\gcd(1001,1331) = \gcd(1001,330) = \gcd(330,11) = \gcd(11,0) = 11$

d) $\gcd(12345,54321) = \gcd(12345,4941) = \gcd(4941,2463) = \gcd(2463,15) = \gcd(15,3) = \gcd(3,0) = 3$

e) $\gcd(1000,5040) = \gcd(1000,40) = \gcd(40,0) = 40$

f) $\gcd(9888,6060) = \gcd(6060,3828) = \gcd(3828,2232) = \gcd(2232,1596) = \gcd(1596,636) = \gcd(636,324)$
$= \gcd(324,312) = \gcd(312,12) = \gcd(12,0) = 12$

Lecture 7

Find gcd(92928, 123552) and lcm(92928, 123552), and verify that $\gcd(92928, 123552) \cdot \mathrm{lcm}(92928, 123552) = 92928 \cdot 123552$. [*Hint:* First find the prime factorizations of 92928 and 123552.]

First we find the prime factorizations: $92928 = 2^8 \cdot 3 \cdot 11^2$ and $123552 = 2^5 \cdot 3^3 \cdot 11 \cdot 13$. Therefore $\gcd(92928, 123552) = 2^5 \cdot 3 \cdot 11 = 1056$ and $\mathrm{lcm}(92928, 123552) = 2^8 \cdot 3^3 \cdot 11^2 \cdot 13 = 10872576$. The requested products are $(2^5 \cdot 3 \cdot 11) \cdot (2^8 \cdot 3^3 \cdot 11^2 \cdot 13)$ and $(2^8 \cdot 3 \cdot 11^2) \cdot (2^5 \cdot 3^3 \cdot 11 \cdot 13)$, both of which are $2^{13} \cdot 3^4 \cdot 11^3 \cdot 13 = 11{,}481{,}440{,}256$.

Lecture 7

Lecture 7