DIVISIBILITY AND MODULARITY

CONGRUENCY

- Definition: Congruent to b modulo m. Let $a, b, m \in \mathbb{Z}$. We say that a is congruent to b modulo m denoted

$$a \cong b \bmod m$$

- iff $m|(a - b)$

EXAMPLE 6

- Determine which of the following is true?

  a) $7 \cong 3(\bmod 4)$
     - $4|(7-3) \rightarrow 4|4 \Longrightarrow TRUE$

  b) $15 \cong 5(\bmod 2)$
     - $2|(15-5) \rightarrow 2|10 \Longrightarrow TRUE$

  c) $15 \cong 3(\bmod 2)$
     - $2|(15-3) \rightarrow 2|12 \Longrightarrow TRUE$

  d) $15 \cong 3(\bmod 5)$
     - $5|(15-3) \rightarrow 5|12 \Longrightarrow FALSE$

THEOREM 4.1.3

- Let $a, b \in \mathbb{Z}, m \in \mathbb{Z}^+$
- Then $a \cong b(\text{mod } m) \Leftrightarrow a \text{ mod } m \cong b \text{ mod } m$
- Proof:
- WTS: $a \cong b(\text{mod } m) \rightarrow a\ (\text{mod } m) = b(\text{mod } m)$
- By assumption $a \cong b(\text{mod } m)$. Hence $\exists k \in \mathbb{Z}$ such that $a - b = m \times k$
- Note: the remainder is 0 when $a - b$ is divided by m
- By division algorithm, $\exists q_1, q_2, r_1, r_2 \in \mathbb{Z}$
- $a = m \times q_1 + r_1, b = m \times q_2 + r_2$
- $a - b = (m \cdot q_1 + r_1) - (m \cdot q_2 + r_2) = m(q_1 - q_2) + r_1 - r_2 = m \cdot u - s$
- Where $u = q_1 - q_2 \in \mathbb{Z}$ and $s = r_1 - r_2 \in \mathbb{Z}$
- So then, $m|(a - b) \rightarrow$ the remainder must be $0 \rightarrow s = 0 \rightarrow r_1 - r_2 = 0 \rightarrow r_1 = r_2$
- Since, $a = m \cdot q_1 + r_1 \rightarrow r_1 = a(mod\ m)$ and $b = m \cdot q_2 + r_2 \rightarrow r_2 = b(mod\ m)$
- Hence, $a(\text{mod } m) = b(\text{mod } m)$

THEOREM 4.1.4

- Let $m \in \mathbb{Z}^{+}$. If $a \cong b(\mathrm{mod}\ m)$ and $c \cong d(\mathrm{mod}\ m)$ then
  - *i.* $a + c \cong b + d(\mathrm{mod}\ m)$
  - *ii.* $ac \cong bd(\mathrm{mod}\ m)$
- Proof:

i. WTS: $a + c \cong b + d(\mathrm{mod}\ m)$

- Since $a \cong b(mod\ m), \exists k_1 | (a - b) \equiv mk_1 \rightarrow a = mk_1 + b$
- Since c$\cong d(mod\ m), \exists k_2 | (c - d) \equiv mk_2 \rightarrow c = mk_2 + d$
- $a + c = (mk_1 + b) + (mk_2 + d) = m(k_1 + k_2) + (b + d)$
- $a + c = mk + (b + d)$ where $k = k_1 + k_2 \in \mathbb{Z}$
- $\rightarrow (a + c) - (b + d) = mk \rightarrow m | (a + c) - (b + d)$
- By definition of congruency, $a + c \cong b + d(\mathrm{mod}\ m)$

THEOREM 4.1.4

- Let $m \in \mathbb{Z}^+$. If $a \cong b(\text{mod } m)$ and $c \cong d(\text{mod } m)$ then
  i. $a + c \cong b + d(\text{mod } m)$
  ii. $ac \cong bd(\text{mod } m)$
- Proof:

ii. WTS: $ac \cong bd(\text{mod } m)$
  - $a \equiv b(mod\ m) \rightarrow \exists k_1 \in \mathbb{Z}, a - b \equiv mk_1 \rightarrow a = mk_1 + b$
  - $c \equiv d(mod\ m) \rightarrow \exists k_2 \in \mathbb{Z}, c - d \equiv mk_2 \rightarrow c = mk_2 + d$
  - $ac = (mk_1 + b)(mk_2 + d) = m^2k_1k_2 + mk_1d + mk_2b + bd$
  - $ac = m(mk_1k_2 + k_1d + k_2b) + bd = mq + bd$ where $q \in \mathbb{Z} \rightarrow ac - bd = mq$
  - By definition of congruency, $ac \equiv bc(\text{mod } m)$

COROLLARY 4.1.4

- Let $m \in \mathbb{Z}^+$,

i. $(a + b) \bmod m = |a \bmod m + b \bmod m| \bmod m$

ii. $(a \cdot b) \bmod m = |(a \bmod m)(b \bmod m)| \bmod m$

EXAMPLE 7

- Find the following without using a calculator
$$(3^4 \text{mod } 17)^2 \text{mod } 11$$
- Let $B = 3^4 \text{mod } 17$ so that our goal is to compute $B^2 mod\ 11$. What is B?
- $B = 3^4 \text{mod } 17 = 81 \text{ mod } 17 = 13$ because $81 = 17 \cdot 4 + 13$
- So then, $B^2 mod\ 11 = 13^2 \text{mod } 11$
- By cor 4.1.4 $B^2 \text{ mod } 11 = |(13 \text{ mod } 11)(13 \text{ mod } 11)| \text{mod } 11$
- $B^2 \text{ mod } 11 = |2 \cdot 2| \text{mod } 11 = 4 \text{ mod } 11 = 4$

INTEGERS MODULO m_1 $\mathbb{Z}_m$

- Definition: The integers modulo m, denotes $\mathbb{Z}_m$, are defined to be
$$\mathbb{Z} = 0,1,2, \dots, m-1$$
- e.g. $\mathbb{Z}_5 = 0,1,2,3,4$
- Operations:
  - $a +_m b = (a+b) \bmod m$
  - $a \cdot_m b = a \cdot b \bmod m$

EXAMPLE 8

- Find the following

a) $7_{11} + 9 = (7 + 9) mod\ 11$

- $7_{11} + 9 = 16\ mod\ 11 = 5 \rightarrow 16 = 1 \cdot 11 + 5$

b) $7_{11} \times 9 = (7 \cdot 9) mod\ 11$

- $7_{11} \times 9 = 63\ mod\ 11 = 8 \rightarrow 63 = 11 \times 5 + 8$

PRIMES AND GCD

PRIME/COMPOSITE

- Definition: Any integer $p > 1$ is a prime number if its only factors are 1 and itself
- e.g. 3, 5, 7, 11, 13
- An integer is composite if it is not prime

THEOREM 4.3.1

- Every composite number has a unique prime factorization

$$c = P_0^{a_0} \times P_1^{a_1} \times \cdots \times P_K^{a_K}$$

- e.g. $100 = 25 \times 4 = 5^2 \times 2^2$

THEOREM 4.3.2

- If n is a composite number $\exists p \leq \sqrt{n}$ such that p is prime and $p|n$
- e.g. $n = 82 \; \exists p \leq \sqrt{82}$\approx 9
- Primes: 2, 3, 5, 7 (all are less than 9)

PROOF OF THEOREM 4.3.2

- Suppose n is a composite $\exists a, b \in \mathbb{Z}$ such that $1 < a, b < n$ and $n = a \times b$ i.e. a and b are factors of n
- Case 1: $a > \sqrt{n}$ and $b > \sqrt{n}$
- Then $a \times b > \sqrt{n} \times \sqrt{n} = n \rightarrow$ This is NOT possible
- Case 2: $a > \sqrt{n}$ or $b > \sqrt{n}$
- WLOE: Assume $a \leq \sqrt{n}$
- Case i: a is composite
- Then a has a unique prime factorization $a = P_0^{a_0} \times P_1^{a_1} \times \cdots \times P_n^{a_n}$
- Then $P_0 | a$ and since $a | n \rightarrow P_0 | n \rightarrow \exists P_0 \leq \sqrt{n}$ and it divides n
- Case ii: a is prime $\rightarrow a \leq \sqrt{n}$ and $a | n$
- Therefore $\exists a \leq \sqrt{n}$ that divides n

EXAMPLE 1

- Show that 61 is prime
- Assume that 61 is composite. Then by Theorem 4.3.2 there must exist some prime $p \leq \sqrt{61}$ that divides 61
- Primes in range [1,8]: 2, 3, 5, 7 → $2 \nmid 61, 3 \nmid 61, 5 \nmid 61, 7 \nmid 61$
- Therefore, our assumption must be wrong. 61 is actually prime

TRIAL DIVISION ALGORITHM

- Goal: Find prime factorization of a composite number
- Let $n \in \mathbb{Z}^+$ be a composite integer
- (1) Divide nb by successive primes starting with $P = 2$
- (2) If $n = k \times P$ (i.e. $P|n$) then
  - a) k is prime $\rightarrow n = k \times P$ is the prime factorization
  - b) k is composite and has a prime factorization itself $\rightarrow$ Find prime factorization of k in the same manner (i.e. divide by successive primes)
  - c) If $!\exists\ p$ such that $p|n$ and $p \leq \sqrt{n}$ then n is already prime

EXAMPLE: TRIAL DIVISION ALGORITHM

- Let $n = 15$
- $p = 2|15?$ No
- $p = 3|15?$ Yes, $15 = 5 \times 3$
- $k = 5$: is k composite?
- If k is composite $\exists p \leq \sqrt{5}$ such that $p|5$, since 2 is the only prime that is $\leq \sqrt{5}$ and $2 \nmid 5$ then k is not composite. Hence $15 = 5 \times 3$ is the prime factorization

GCD

- Definition: Let $a, b \in \mathbb{Z}^+$. The largest $d \in \mathbb{Z}^+$ such that $d|a$ and $d|b$ is called the greatest common divisor (GCD)

$$d = \gcd(a, b)$$

EXAMPLE 2

- Give the GCD of the following:

a) 24 and 32
  - 24: 1, 2, 3, 4, 6, 8, 12, 24
  - 32: 1, 2, 4, 8
  - $\gcd(24, 36) = 8$

b) 13 and 24
  - 13: 1, 13
  - 24: 1, 2, 3, 4, 6, 8, 12, 24
  - $\gcd(13,24) = 1$

RELATIVELY PRIME

- Definition: Two or more integers are relatively prime if their gcd is 1

EXAMPLE 3

- Determine if the set of numbers are relatively prime:

a) 8, 13, 21
   - gcd(8,13)=1
   - gcd(13,21)=1
   - Yes

b) 10, 18, 23
   - gcd(10,18)=2
   - gcd(18,23)=1
   - No

GCD ALGORITHM

- Devise an algorithm to find the gcd of any two numbers
- E.g. $24 = 3 \times 8 = 3 \times 2^3$
- $36 = 3 \times 12 = 3^2 + 2^2$
- $\gcd(24, 36) = 12 = (2^2 \times 3)$
- $\rightarrow$ The gcd is the product of the smallest power of the factors present in the prime factorization
- In general: if $a = P_1^{a_1} \times P_2^{a_2} \times \cdots \times P_n^{a_n}$ and $b = P_1^{b_1} \times P_2^{b_2} \times \cdots \times P_n^{b_n}$
- Then $\gcd(a, b) = P_1^{\min(a_1, b_1)} \times P_2^{\min(a_1, b_1)} \times \cdots \times P_n^{\min(a_n, b_n)}$

EXAMPLE 4

- Find the GCD of 120 and 500
- $120 = 2^3 \times 3 \times 5$
- $500 = 2^2 \times 3^0 \times 5^3$
- $\gcd(120, 500) = 2^2 \times 3^0 \times 5^1 = 20$

LCM

- Definition: Let $a, b \in \mathbb{Z}^+$. The least common multiple of a and b is the smallest $m \in \mathbb{Z}$ such that $a|m$ and $b|m$

$$lcm(a, b) = m$$

EXAMPLE 5

- Find the LCM of the following:

a) 8, and 10
   - 10: 10, 20, 30, 40
   - $\mathrm{lcm}(10,8) = 40$ because 10 divides 40 and 8 divides 40

b) 100 and 54
   a) 100: $2^2 \times 5^2$
   b) 54: 2×27
   c) $\mathrm{lcm}(100,54) = 2^2 \times 5^2 \times 27 = 2700$

LCM ALGORITHM

- In general: if $a = P_1^{a_1} \times P_2^{a_2} \times \cdots \times P_n^{a_n}$ and $b = P_1^{b_1} \times P_2^{b_2} \times \cdots \times P_n^{b_n}$
- Then $\operatorname{lcm}(a, b) = P_1^{\max(a_1,b_1)} \times P_2^{\max(a_1,b_1)} \times \cdots \times P_n^{max(a_n,b_n)}$

THEOREM 4.3.3

- Let $a, b \in \mathbb{Z}^+ : a \times b = \gcd(a, b) \times \operatorname{lcm}(a, b)$
- So far we have found the GCD by prime factorization. This is known as the trial Division Algorithm. However, in practice it takes too long to find prime factorizations, instead consider the Euclidean Algorithm

EUCLIDEAN ALGORITHM EXAMPLE

- Motivation: Suppose we wish to find the $\gcd(24,36)$. We know that whatever is is, it must divide 36 and 24
- $36 = 1 \times 24 + 12$
- $24 = 2 \times 12 + 0$
- $36 = 2 \times 12 + 12$
- Hence, the gcd is 12 because it divides both

THEOREM 4.3.4

- Let $a, b \in \mathbb{Z}^+ : a \times b = \gcd(a, b) \times lcm(a, b)$
- Then $\gcd(a, b) = \gcd(b, r)$ where r is the remainder of a/b and $b \leq a$
- Idea: show that all the divisions of a with b are also divisors of b with r
- i.e. $\forall d \in \mathbb{Z}^+ \; d|a \; AND \; d|b \;\; \Leftrightarrow d|b \; AND \; d|r$

PROOF OF THEOREM 4.3.4

- $\Rightarrow$ Suppose $d|a$ and $d|b$
- Then $a = d \times k, k \in \mathbb{Z}$ and $b = d \times y, y \in \mathbb{Z}$
- $a = bq + r$ by assumption
- So then $r = a - bq = dk - dyq = d(k - yq) = du, u \in \mathbb{Z}$
- So then $d|r$, which means that $d|b$ and $d|r$
- $\Leftarrow$ Suppose $d|b$ and $d|r$
- Then $b = d \times y, y \in \mathbb{Z}$ and $r = d \times z, z \in \mathbb{Z}$
- Since $a = bq + r$ by assumption
- Then $a = dyq + dz = d(yq + z) = dt, t \in \mathbb{Z}$
- So then $d|a$, which means that $d|a$ and $d|b$

EXAMPLE 6

- Find the GCD of the following using theorem 4.3.4

a) $\gcd(120,500)$

  - $\gcd(120,500)$=gcd(120, 20)=20
  - $500 = 4 \times 120 + 20$
  - $120 = 6 \times 20 + 0$

b) $\gcd(414,662)$

  - $\gcd(414,662) = \gcd(414,248) = \gcd(248,166) = \gcd(166,82) = \gcd(82,2) = 2$

- Claim: The gcd will be the last non zero remainder of the division algorithm process

PSEUDOCODE: EUCLIDEAN ALGORITHM

- Input: a, b integers
- Output: y=gcd(x,y)
- gcd(a,b)
    - x=max(a,b)
    - y=min(a,b)
    - r=x mod y
- while r != 0:
    - x=y
    - y=r
    - r = x mod y
- return y

THEOREM 4.3.5

- Let $a, b \in \mathbb{Z}^+$ then $\exists s, t \in \mathbb{Z}$ such that $\gcd(a, b) = sa + tb$. The integer s and t are called Bezout Coefficients

EXAMPLE 7

- Find the Bezout Identity for the following:

a) $\gcd(120{,}500)$

- $500 = 4 \times 120 + 20 \rightarrow 120 = 6 \times 20 + 0 \rightarrow 20 = 500 - 4 \times 120$
- $(s, t) = (1, -4)$

b) $\gcd(414{,}662)$

- $\gcd(414{,}662) = 2 \rightarrow 2 = 8 \times 414 - 5 \times 662$
- $(s, t) = (8, -5)$

EXAMPLE 7 (EXPANDED)

- $\gcd(414{,}662) = 2$
- $662 = 1 \cdot 414 + 248 \rightarrow 248 = 662 - 414$
- $414 = 1 \cdot 248 + 166 \rightarrow 166 = 414 - 248$
- $248 = 1 \cdot 166 + 82 \rightarrow 82 = 248 - 166$
- $166 = 2 \cdot 82 + 2 \rightarrow 2 = 166 - 2 \cdot 82$ (solve for remainder $\uparrow$)
- $82 = 41 \cdot 2 + 0$
- $2 = 166 - 2(248 - 166) = 3 \cdot 166 - 2 \cdot 248$ (simplify equation)
- $2 = 3 \cdot (414 - 248) - 2 \cdot 248 = 3 \cdot 414 - 5 \cdot 248$
- $2 = 3 \cdot 414 - 5(661 - 414) = 8 \cdot 414 - 5 \cdot 661$