L06: GCDs and Congruences

- **Greatest Common Divisor (GCD)**
- Multiplicative Inverses
- Solving Linear Congruences
- The Chinese Remainder Theorem

- Reading: Rosen 4.3, 4.4, 4.5

Review of Primary School Knowledge

- **Definition**
  A positive 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*.
- **Theorem** (The Fundamental Theorem of Arithmetic)
  Every positive 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.
  (Will prove later by induction)

Greatest Common Divisor

- **Definition**
  Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and also $d \mid b$ is called the greatest common divisor of a and b, denoted by $\gcd(a, b)$.
- One can find the gcd by prime factorizations
- **Example**
  $120 = 2^3 \cdot 3 \cdot 5 \qquad 500 = 2^2 \cdot 5^3$
  $\gcd(120{,}500) = 2^{\min(3,2)} \cdot 3^{\min(1,0)} \cdot 5^{\min(1,3)} = 2^2 \cdot 3^0 \cdot 5^1 = 20$
- **Definition**
  The integers a and b are relatively prime if $\gcd(a, b) = 1$.
  - Example: 17 and 22

Euclidean Algorithm

- However, factoring large numbers is hard!
  - No efficient algorithms exist
- **Lemma**
  Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.
- **Proof**
  - Suppose that d divides both a and b. Then d also divides $a - bq = r$. Hence, any common divisor of a and b must also be any common divisor of b and r.
  - Suppose that d divides both b and r. Then d also divides $bq + r = a$. Hence, any common divisor of b and r must also be a common divisor of b and a.
  - Therefore, $\gcd(a, b) = \gcd(b, r)$.

Euclidean Algorithm

- Idea: To obtain maximum efficiency, choose the smallest r, i.e., $r = a \bmod b$ (suppose $a > b$), and iterate.

```
gcd(a,b):
x ← $a$
y ← $b$
while $y \neq 0$
    $r \leftarrow x \bmod y$
    $x \leftarrow y$
    $y \leftarrow r$
return $x$
```

Example:

$$
\begin{aligned}
&\gcd(287, 91)\\
&= \gcd(91, 14)\\
&= \gcd(14, 7)\\
&= \gcd(7, 0)\\
&= 7
\end{aligned}
$$

- Correctness of algorithm follows from previous lemma
- Termination is obvious
- Running time will be analyzed later

gcds as Linear Combinations

- **Theorem** (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
  $$\gcd(6,14) = (-2) \cdot 6 + 1 \cdot 14$$
- Instead of proving this theorem directly, we give an algorithm to find such s and t.

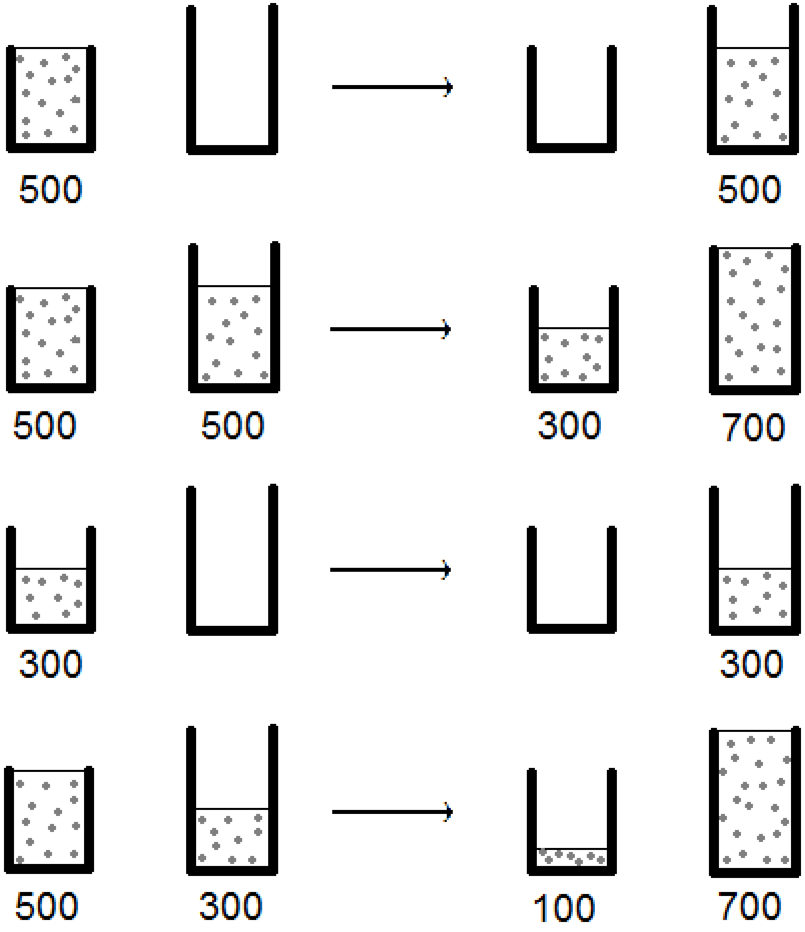
The Extended Euclidean Algorithm

- **Example**
  Express $\gcd(252,198)$ as a linear combination of 252 and 198.
- **Solution**
  - First find $\gcd(252,198)$
    1) $252 = 1 \cdot 198 + 54$
    2) $198 = 3 \cdot 54 + 36$
    3) $54 = 1 \cdot 36 + 18$
    4) $36 = 2 \cdot 18$
    5) $\gcd(252,198) = 18$
  - Rewriting:
    - $54 = 252 - 1 \cdot 198$
    - $36 = 198 - 3 \cdot 54$
    - $18 = 54 - 1 \cdot 36$
  - Substituting:

$$
\begin{aligned}
18 &= 54 - 1 \cdot (198 - 3 \cdot 54) \\
&= 4 \cdot 54 - 1 \cdot 198 \\
&= 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 \\
&= 4 \cdot 252 - 5 \cdot 198
\end{aligned}
$$

Puzzle: Water Measuring

- Given
  - Two bottles: one has volume of 500 ml and the other one 700 ml.
  - Infinite water supply
- Goal: Get exactly 100 ml of water
- This follows exactly from
  $$100 = \gcd(500,700)$$
  $$= 3 \times 500 - 2 \times 700$$
- Corollary: Any multiple of the gcd can be obtained.



Outline

- Greatest Common Divisor (GCD)
- **Multiplicative Inverses**
- Solving Linear Congruences
- The Chinese Remainder Theorem

Multiplicative Inverses

- **Definition**
  The (multiplicative) inverse of a modulo m is some b such that $ab \equiv 1 \pmod{m}$.
- By default “inverse” means “multiplicative inverse”.
- **Examples**

$\mathbf{Z}_5$:

a	1	2	3	4
a^{-1}	1	3	2	4

$\mathbf{Z}_7$:

a	1	2	3	4	5	6
a^{-1}	1	4	5	2	3	6

$\mathbf{Z}_6$:

a	1	2	3	4	5
a^{-1}	1	X	X	X	5

$\mathbf{Z}_8$:

a	1	2	3	4	5	6	7
a^{-1}	1	X	3	X	5	X	7

Multiplicative Inverses

- **Theorem**
  For any $a \in \mathbf{Z}_m, m > 1$, if $\gcd(a, m) = 1$ then a has a unique inverse in $\mathbf{Z}_m$.
- **Corollary**
  For any prime p, every nonzero $a \in \mathbf{Z}_p$ has a multiplicative inverse.
- **Proof of Theorem**
  Since $\gcd(a, m) = 1$, by Bézout's Theorem, there are integers *s* and *t* such that $sa + tm = 1$.
  - Hence, $sa = (-t)m + 1$
  - Since $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$.
  - Since *s* may not be in $\mathbf{Z}_m$, we write $(s \bmod m) \cdot_m a = 1$
  - Consequently, *s* mod *m* is the inverse of *a* in $\mathbf{Z}_m$.

Multiplicative Inverses are Unique

- **Proof of uniqueness**
  - Suppose b, c are both inverses of a, i.e.,

$$ab \equiv 1 \pmod{m} \qquad (1)$$

$$ac \equiv 1 \pmod{m} \qquad (2)$$

  - Multiply both sides of (1) by c:

$$abc \equiv c \pmod{m}$$

  - Multiply both sides of (2) by b:

$$abc \equiv b \pmod{m}$$

  - So $b \equiv c \pmod{m}$, i.e., a has a unique inverse in $\mathbf{Z}_m$.
- The inverse of a is written as a^{-1}.
- Note: It's also true that if $\mathrm{gcd}(a, m) \neq 1$, a^{-1} doesn't exist. (Left as an exercise.)

Finding Inverses

- Given a, m such that $\gcd(a, m) = 1$, how to find the inverse of a in $\mathbf{Z}_m$?
- Look at the proof of the previous theorem
  - Use the extended Euclidean algorithm to find s and t such that $sa + tm = 1$
  - s mod m is the multiplicative inverse of a in $\mathbf{Z}_m$.
- **Example**
  Find an inverse of 3 modulo 7
- **Solution**
  Using the extended Euclidean algorithm: $7 = 2{\cdot}3 + 1$.
  we get $-2{\cdot}3 + 1{\cdot}7 = 1$, so $s = -2$.
  $-2 \bmod 7 = 5$ is the inverse of 3 in $\mathbf{Z}_7$

Finding Inverses

- **Example**
  Find the inverse of 101 modulo 4620

$$4620 = 45 \cdot 101 + 75$$
$$101 = 1 \cdot 75 + 26$$
$$75 = 2 \cdot 26 + 23$$
$$26 = 1 \cdot 23 + 3$$
$$23 = 7 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1$$

Since the last nonzero remainder is 1, gcd(101,4620) = 1

Working Backwards:

$$1 = 3 - 1 \cdot 2$$
$$1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$$
$$1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$$
$$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$$
$$1 = 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75$$
$$= 26 \cdot 101 - 35 \cdot 75$$
$$1 = 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101)$$
$$= -35 \cdot 4620 + 1601 \cdot 101$$

1601 is an inverse of 101 modulo 4620

Outline

- Greatest Common Divisor (GCD)
- Multiplicative Inverses
- **Solving Linear Congruences**
- The Chinese Remainder Theorem

Solving Congruences

- Linear congruence

$$ax \equiv b \pmod{m}$$

- Given a, b, m, such that $\gcd(a, m) = 1$. How to find x?
- Solution:
  - Find a^{-1}
  - Multiply a^{-1} on both sides
- Example
  - Solve $3x \equiv 4 \pmod{7}$
  - Find $3^{-1} = 5$
  - Multiply 5 on both sides:

$$3^{-1} \cdot 3x \equiv 3^{-1} \cdot 4 \pmod{7}$$

$$x \equiv 5 \quad 4 \equiv 6 \pmod{7}$$

Solving Congruences

- **Corollary**
  If $\gcd(a, m) = 1$, the linear congruence
  $$ax \equiv b \pmod{m}$$
  has a unique solution in $\mathbf{Z}_m$
- **Proof**
  - Existence has already been proved by construction.
  - Uniqueness: Suppose it has two solutions x_1, x_2:
    $$ax_1 \equiv b \pmod{m}$$
    $$ax_2 \equiv b \pmod{m}$$
    Multiply both by a^{-1}:
    $$x_1 \equiv ba^{-1} \pmod{m}$$
    $$x_2 \equiv ba^{-1} \pmod{m}$$
    So, $x_1 \equiv x_2 \pmod{m}$.

Solving congruences

- Note: If $\gcd(a, m) \neq 1$, the linear congruence
$$ax \equiv b \pmod{m}$$
may have no solution or multiple solutions in $\mathbf{Z}_m$

Examples:

- $2x \equiv 1 \pmod{6}$ has no solution in $\mathbf{Z}_6$
- $2x \equiv 4 \pmod{6}$ has two solutions in $\mathbf{Z}_6$
$$x = 2, 5$$

Revisiting the String Hash Function

- Consider the case with only 3 characters:

$$h(s) = \Big(\big((s[0] \cdot 31 + s[1]) \cdot 31 + s[2]\big) \bmod 2^{32}\Big) \bmod n$$

- Note $\gcd(31, 2^{32}) = 1$
- Given any $s[2]$ and b, the congruence

  $$31x + s[2] \equiv b \pmod{2^{32}}$$

  has a unique solution. This means, given $s[2]$, $h(s)$ depends on $x = s[0] \cdot 31 + s[1]$ and every b is possible.
- Similarly, given any $s[1]$, x can possibly take any value depending on $s[0]$.
- Other reasons:
  - Performance: x*31 = x << 5 – x
  - Using 31 produces more balanced hashes over English text

Checksums

- **Example**
  HKID numbers are of the format X123456(Y), where
  - X is one or two letters
  - Y is check digit, 0 to 9 or A.
- **How is it computed**
  - Replace the first two letters as follows:
    A = 10 B = 11 C = 12 D = 13 E = 14 F = 15 G = 16 H = 17 I = 18 J = 19
    K = 20 L = 21 M = 22 N = 23 O = 24 P = 25 Q = 26 R = 27 S = 28
    T = 29 U = 30 V = 31 W = 32 X = 33 Y = 34 Z = 35 empty = 36
  - Denote the resulting two numbers and 6 digits as $x_1, \dots, x_8$
  - $c = (9x_1 + 8x_2 + 7x_3 + 6x_4 + \cdots + 2x_8) \bmod 11$
  - Check digit $x_9 = 11 - c$
    If $x_9 = 11$, check digit = 0
    If $x_9 = 10$, check digit = A

HKID Checksum: Single Error

- Note that for a valid HKID, we have
$$9x_1 + 8x_2 + 7x_3 + \cdots + 2x_8 + x_9 \equiv 0 \pmod{11}$$
- Suppose x_3 is mistyped as $x_3' \neq x_3$
- Suppose the checksum is still correct, i.e.,
$$9x_1 + 8x_2 + 7x_3' + \cdots + 2x_8 + x_9 \equiv 0 \pmod{11}$$
- Subtracting one congruence from the other:
$$7(x_3 - x_3') \equiv 0 \pmod{11}$$
- Since $\gcd(7, 11) = 1$, 7 has an inverse. Multiply both sides by 7^{-1}:
$$x_3 - x_3' \equiv 0 \pmod{11}$$
- This contradicts with the assumption $x_3' \neq x_3$ and they are both in $\{0, \dots, 9\}$
- Note: If first or second letter is wrong, it may not be detected!

HKID Checksum: Transposition Error

- Note that for a valid HKID, we have
$$9x_1 + 8x_2 + 7x_3 + \cdots + 2x_8 + x_9 \equiv 0 \pmod{11}$$
- Suppose x_3 and x_5 are swapped, and $x_3 \neq x_5$
- Suppose the checksum is still correct, i.e.,
$$9x_1 + 8x_2 + 7x_5 + 6x_4 + 5x_3 \ldots + 2x_8 + x_9 \equiv 0 \pmod{11}$$
- Subtracting one congruence from the other:
$$2(x_5 - x_3) \equiv 0 \pmod{11}$$
- Since $\gcd(2, 11) = 1$, 2 has an inverse. Multiply both sides by 2^{-1}:
$$x_5 - x_3 \equiv 0 \pmod{11}$$
- This contradicts with the assumption $x_3 \neq x_5$ and they are both in $\{0, \ldots, 9\}$

Outline

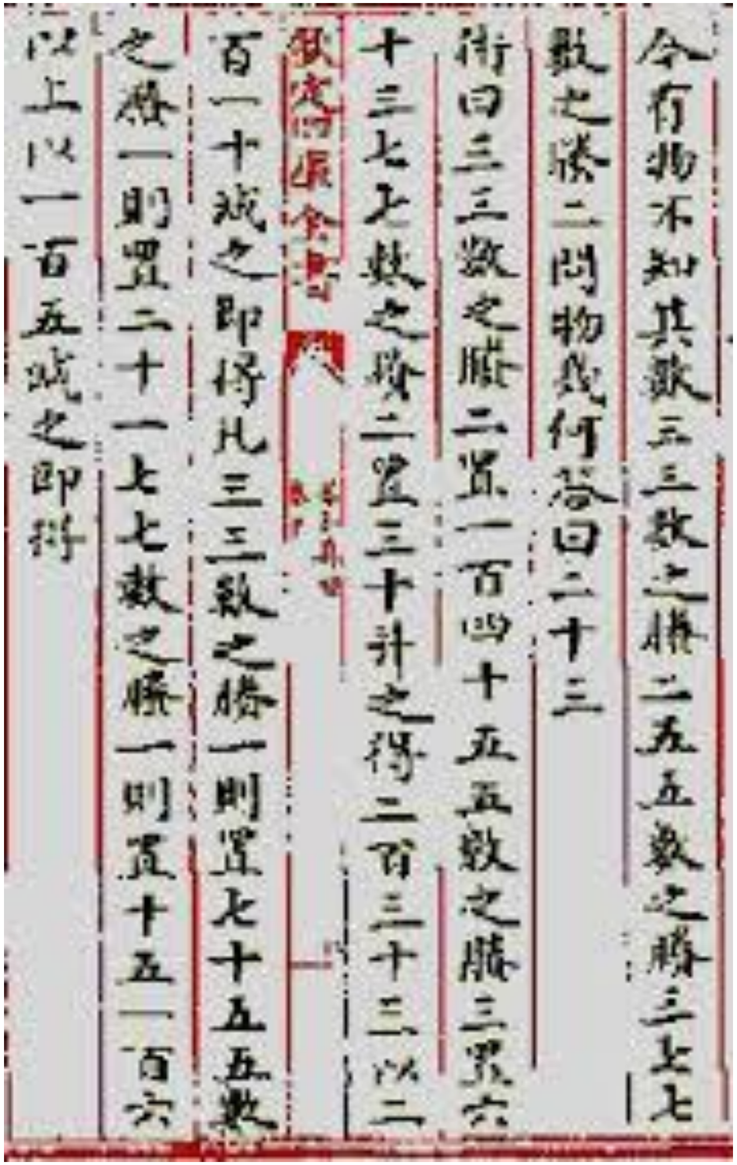
- Greatest Common Divisor (GCD)
- Multiplicative Inverses
- Solving Linear Congruences
- **The Chinese Remainder Theorem**

Sun-Tsu’s Problem

There are certain things whose number is unknown. If we count them by threes, we have two left over; by fives, we have three left over; and by sevens, two are left over. How many things are there?

System of linear congruences:

$$x \equiv 2 \pmod{3},$$
$$x \equiv 3 \pmod{5},$$
$$x \equiv 2 \pmod{7}.$$



今有物不知其數三三數之賸二五五數之賸三七七
數之賸二問物幾何答曰二十三
術曰三三數之賸二置一百四十五五數之賸三置六
十三七七數之賸二置三十并之得二百三十三以二
欽定四庫全書
百一十減之即得凡三三數之賸一則置七十五五數
之賸一則置二十一七七數之賸一則置十五一百六
以上以一百五減之即得

The Chinese Remainder Theorem

- **Theorem**
  Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$\begin{gathered} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \ldots \\ x \equiv a_n \pmod{m_n} \end{gathered}$$

  has a unique solution modulo $m = m_1 m_2 \cdots m_n$.
- **Proof**
  We'll show that a solution exists by describing a way to construct the solution. (Uniqueness proof is left as exercise.)

The Chinese Remainder Theorem

- **Proof**

  Let $M_k = \frac{m}{m_k}, k = 1,2, \dots, n$

  Since $\gcd(m_k, M_k) = 1, M_k$ has an inverse y_k modulo m_k:

  $$M_k y_k \equiv 1 \pmod{m_k}$$

  We claim that this is a solution:

  $$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$$

  Check:

  $$x \equiv a_k \pmod{m_k}?$$

  $M_j \equiv 0 \pmod{m_k}$ if $j \neq k$ $\Rightarrow$ $a_j M_j y_j \equiv 0 \pmod{m_k}$ if $j \neq k$;

  $M_k y_k \equiv 1 \pmod{m_k}$ $\Rightarrow$ $a_k M_k y_k \equiv a_k \pmod{m_k}$

The Chinese Remainder Theorem

- Consider the 3 congruences from Sun-Tsu's problem:

  $x \equiv 2 \pmod{3}, \; x \equiv 3 \pmod{5}, \quad x \equiv 2 \pmod{7}.$
- Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, $M_3 = \; m/7 = \; 15$.
- We see that
  - 2 is an inverse of $M_1 \pmod{3}$
  - 1 is an inverse of $M_2 \pmod{5}$
  - 1 is an inverse of $M_3 \pmod{7}$
- Hence,

$$\begin{aligned} x &= a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \\ &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105} \end{aligned}$$