# Number Theory and Cryptography

Chapter 4

With Question/Answer Animations

# Chapter Summary

4.1 Divisibility and Modular Arithmetic

4.2 Integer Representations and Algorithms

4.3 Primes and Greatest Common Divisors

**4.4 Solving Congruences**

4.5 Applications of Congruences

4.6 Cryptography

# Solving Congruences

Section 4.4

# Section Summary

- Linear Congruences
- The Chinese Remainder Theorem
- Computer Arithmetic with Large Integers (*not in slides, see text*)
- Fermat's Little Theorem
- Pseudoprimes
- Primitive Roots and Discrete Logarithms

# Linear Congruences

**Definition**: A congruence of the form

$$ax \equiv b(\bmod m),$$

where $m \in Z^+$, $a$, $b \in Z$, and $x$ is a variable, is a *linear congruence*.

- Solutions to $ax \equiv b(\bmod m)$ are $x \in Z$ that satisfy congruence.

**Definition**: $\bar{a} \in Z$ such that $\bar{a}a \equiv 1(\bmod m)$ is an *inverse* of $a$ mod $m$.
**Example**: 5 is an inverse of 3 mod 7 since $5 \cdot 3 = 15 \equiv 1 (\text{mod } 7)$

- One method of solving linear congruences uses inverse $\bar{a}$, if it exists.
- Although we can not divide both sides of the congruence by $a$,
  - we can multiply by $\bar{a}$ to solve for $x$.

# Inverse of *a* modulo *m*

**Theorem 1**: If $a$ and $m$ are relatively prime integers, $m > 1$, then an inverse of $a$ mod $m$ exists. Furthermore, this inverse is unique modulo $m$.

( i.e., $\exists! \bar{a} \in 1, \ldots, m-1$ that is an inverse of $a$ mod $m$ and every other inverse of $a$ mod $m$ is congruent to $\bar{a}$ mod $m$.)

**Proof**: Since $\gcd(a, m) = 1$, by Theorem 6 of Section 4.3,

$\exists s, t$ such that $sa + tm = 1$ (Bézout coefficients)

- Hence, $sa + tm \equiv 1 \pmod{m}$.
- Since $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$
- Consequently, $s$ is an inverse of $a$ modulo $m$.
- The uniqueness of the inverse is Exercise 7.

# Finding Inverses

The Euclidean algorithm and Bézout coefficients gives us a systematic approaches to finding inverses.

**Example**: Find an inverse of 3 modulo 7.

**Solution**: Because gcd(3,7) = 1, by Theorem 1, an inverse of 3 modulo 7 exists.

- Using the Euclidian algorithm: $7 = 2\cdot3 + 1$.
- From this equation, we get $-2\cdot3 + 1\cdot7 = 1$, and see that $-2$ and 1 are Bézout coefficients of 3 and 7.
- Hence, $-2$ is an inverse of 3 modulo 7.
- Any integer $\equiv$ mod 7 is an inverse of 3 mod 7:
  - $\ldots, -16, -2, -9, 5, 12, \ldots$

# Finding Inverses

**Example**: Find an inverse of 101 modulo 4620.

**Solution**: First use the Euclidian algorithm to show that gcd(101,4620) = 1.

$42620 = 45 \cdot 101 + 75$
$101 = 1 \cdot 75 + 26$
$75 = 2 \cdot 26 + 23$
$26 = 1 \cdot 23 + 3$
$23 = 7 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1$

Since the last nonzero remainder is 1, gcd(101,4260) = 1

Working Backwards:

$1 = 3 - 1 \cdot 2$
$1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$
$1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$
$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$
$1 = 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75$
$= 26 \cdot 101 - 35 \cdot 75$
$1 = 26 \cdot 101 - 35 \cdot (42620 - 45 \cdot 101)$
$= -35 \cdot 42620 + 1601 \cdot 101$

Bézout coefficients : $-35$ and 1601

1601 is an inverse of 101 modulo 42620

# Using Inverses to Solve Congruences

We can solve $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$.

**Example**: Solve $3x \equiv 4 \pmod{7}$

**Solution**: We found that $-2$ is an inverse of 3 modulo 7 (two slides back). Multiply both sides of by $-2$ giving

$$-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7}.$$

Because $-6 \equiv 1 \pmod{7}$ and $-8 \equiv 6 \pmod{7}$, it follows that if $x$ is a solution, then $x \equiv -8 \equiv 6 \pmod{7}$

The solutions are the integers $x$ such that $x \equiv 6 \pmod{7}$, namely,

$$\ldots, -15, -8, -1, 6, 13, 20 \ldots$$

Typically, it would suffice to provide 6, our !representative in 0,…, m-1

# Sun-Tsu's Puzzle

- In the first century, the Chinese mathematician Sun-Tsu asked:

  There are certain things whose number is unknown. When divided by 3, remainder is 2; when divided by 5, remainder is 3; when divided by 7, remainder is 2. What will be the number of things?

- Translate this puzzle into solving a system of congruences:

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

- The *Chinese Remainder Theorem* can be used to solve problem.

# The Chinese Remainder Theorem

**Theorem 2**: (*Chinese Remainder Theorem*) $m_1, m_2, \ldots, m_n \in Z$, >1, pairwise relatively prime (prp), and $a_1, a_2, \ldots, a_n \in Z$, then

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

has a ! solution modulo $m = m_1 m_2 \cdots m_n$.

(That is, ∃ solution x with $0 \leq x < m$ and all other solutions are congruent modulo $m$ to this solution.)

- **Proof**: We'll show that solution exists by describing a way to construct solution. Showing that solution is ! is Exercise 30.

*continued* →

# The Chinese Remainder Theorem

To construct a solution first let $M_k = m/m_k$ for $k = 1,2,\ldots,n$ and $m = m_1 m_2 \cdots m_n$.
Since $\gcd(m_k, M_k) = 1$, by Thm 1, $\exists y_k \in Z$, an inverse of $M_k$ mod $m_k$, such that

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

Form the sum

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

Since $M_j \equiv 0 \pmod{m_k}$ if $j \neq k$, all terms except $k^{th}$ term in sum are $\equiv 0$ mod $m_k$.
Because $M_k\, y_k \equiv 1 \pmod{m_k}$, we see that $x \equiv a_k M_k\, y_k \equiv a_k \pmod{m_k}$, for $k = 1, 2, \ldots, n$.
Hence, $x$ is a simultaneous solution to the $n$ congruences:

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

# The Chinese Remainder Theorem

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

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

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

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

- We have shown that 23 is the smallest positive integer that is a simultaneous solution. Check it!

# Back Substitution

We can also solve systems with pairwise relatively prime moduli by rewriting a ≡ as an equality using Thm 4 of Section 4.1, substituting the value for the variable into another congruence, and continuing the process until we have worked through all congruences. This method is known as *back substitution*.

**Example**: Use the method of back substitution to find all integers $x$ such that

$$x \equiv 1 \pmod{5},\ x \equiv 2 \pmod{6},\ \text{and } x \equiv 3 \pmod{7}.$$

**Solution**: By Thm 4, the first ≡ can be rewritten as $x = 5t + 1$, where $t \in Z$.

- Substituting into the second congruence yields $5t + 1 \equiv 2 \pmod{6}$.
- Solving this tells us that $t \equiv 5 \pmod{6}$.
- Using Theorem 4 again gives $t = 6u + 5$ where $u$ is an integer.
- Substituting this back into $x = 5t + 1$, gives $x = 5(6u + 5) + 1 = 30u + 26$.
- Inserting this into the third equation gives $30u + 26 \equiv 3 \pmod{7}$.
- Solving this congruence tells us that $u \equiv 6 \pmod{7}$.
- By Theorem 4, $u = 7v + 6$, where $v$ is an integer.
- Substituting this expression for $u$ into $x = 30u + 26$, tells us that

  $$x = 30(7v + 6) + 26 = 210u + 206.$$
- Translating this back into a congruence we find solution $x \equiv 206 \pmod{210}$.

Pierre de Fermat (1601-1665)

# Fermat's Little Theorem

**Thm 3**: (*Fermat's Little Thm*) $p$ prime, $a \in Z$, $p \nmid a \Rightarrow a^{p-1} \equiv 1$ **mod** $p$

Furthermore, for every integer $a$ we have $a^p \equiv a \pmod{p}$

(*proof outlined in Exercise 19*)

Fermat's little thm is useful in computing mod $p$ of large powers.

**Example**: Find $7^{222}$ **mod** 11.

By Fermat's little thm, $7^{10} = 1$ **mod** 11, so $(7^{10})^k = 1$ **mod** 11, $\forall k \in Z^+$.

$$\therefore\ 7^{222} = 7^{22\cdot 10 + 2} = (7^{10})^{22} 7^2 \equiv (1)^{22} \cdot 49 = 5 \text{ mod } 11.$$

Hence, $7^{222}$ **mod** $11 = 5$.

# Pseudoprimes

- By Fermat's little theorem $n > 2$ is prime, where
$$2^{n-1} \equiv 1 \pmod{n}.$$
- But if this congruence holds, $n$ may not be prime. Composite integers $n$ such that $2^{n-1} \equiv 1 \pmod{n}$ are *pseudoprimes* to the base 2.

  **Example**: The integer 341 is a pseudoprime to the base 2.

  $341 = 11 \cdot 31$

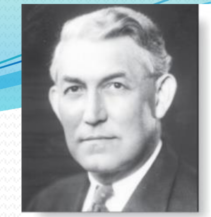
  $2^{340} \equiv 1 \pmod{341}$ (*see in Exercise* 37)
- We can replace 2 by any integer $b \geq 2$.

  **Definition**: Let $b \in Z^+$. If $n$ is composite & $b^{n-1} = 1$ **mod** $n$, then $n$ is a *pseudoprime to the base b*.

# Pseudoprimes

- Given $n \in \mathbb{Z}$, such that $2^{n-1} \equiv 1 \pmod{n}$:
  - If $n$ does not satisfy the congruence, it is composite.
  - If $n$ does satisfy the congruence, it is either prime or a pseudoprime to the base 2.
- Doing similar tests with additional bases $b$, provides more evidence as to whether $n$ is prime.
- Among positive integers not exceeding $x$, $\exists$ relatively few pseudoprimes compared to primes.
  - among the first 10 billion positive #'s,
    - #pseudoprimes to the base 2 ~ 15 k
    - #primes = 455 M

Robert Carmichael (1879-1967)



# Carmichael Numbers(*optional*)

∃composite integers $n$ that pass all tests with bases $b$ such that gcd($b$,$n$) = 1.

**Definition**: A composite integer n that satisfies the congruence $b^{n-1} \equiv 1 \pmod{n}$ $\forall b \in Z^+$ with gcd($b$,$n$) = 1 is a *Carmichael* number.

**Example**: The integer 561 is a Carmichael number. To see this:

- 561 is composite, since 561 = 3 · 11 · 13.
- If gcd($b$, 561) = 1, then gcd($b$, 3) = 1, then gcd($b$, 11) = gcd($b$, 17) =1.
- Using Fermat's Little Theorem: $b^2 \equiv 1 \pmod{3}$, $b^{10} \equiv 1 \pmod{11}$, $b^{16} \equiv 1 \pmod{17}$.
- Then

$$b^{560} = (b^2)^{280} \equiv 1 \pmod{3},$$
$$b^{560} = (b^{10})^{56} \equiv 1 \pmod{11},$$
$$b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}.$$

- It follows (*see Exercise* 29) that $b^{560} \equiv 1 \pmod{561}$ for all positive integers $b$ with gcd($b$,561) = 1. Hence, 561 is a Carmichael number.

- Even though there are infinitely many Carmichael numbers, there are other tests (described in the exercises) that form the basis for efficient probabilistic primality testing. (*see Chapter* 7)

# Primitive Roots (optional)

**Definition**: A primitive root modulo a prime $p$ is an integer $r$ in $\mathbf{Z}_p$ such that every nonzero element of $\mathbf{Z}_p$ is a power of $r$.

**Example**: Since every element of $\mathbf{Z}_{11}$ is a power of 2, 2 is a primitive root of 11.

Powers of 2 modulo 11: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 5$, $2^5 = 10$, $2^6 = 9$, $2^7 = 7$, $2^8 = 3$, $2^{10} = 2$.

**Example**: Since not all elements of $\mathbf{Z}_{11}$ are powers of 3, 3 is not a primitive root of 11.

Powers of 3 modulo 11: $3^1 = 3$, $3^2 = 9$, $3^3 = 5$, $3^4 = 4$, $3^5 = 1$, and the pattern repeats for higher powers.

**Important Fact**: There is a primitive root modulo $p$ for every prime number $p$.

# Discrete Logarithms (optional)

Suppose $p$ is prime and $r$ is a primitive root modulo $p$. If $a$ is an integer between 1 and $p-1$, that is an element of $\mathbf{Z}_p$, there is a unique exponent $e$ such that $r^e = a$ in $\mathbf{Z}_p$, that is, $r^e \bmod p = a$.

**Definition**: Suppose that $p$ is prime, $r$ is a primitive root modulo $p$, and $a$ is an integer between 1 and $p-1$, inclusive. If $r^e \bmod p = a$ and $1 \leq e \leq p-1$, we say that $e$ is the *discrete logarithm* of $a$ modulo $p$ to the base $r$ and we write $\log_r a = e$ (where the prime $p$ is understood).

**Example 1**: We write $\log_2 3 = 8$ since the discrete logarithm of 3 modulo 11 to the base 2 is 8 as $2^8 = 3$ modulo 11.

**Example 2**: We write $\log_2 5 = 4$ since the discrete logarithm of 5 modulo 11 to the base 2 is 4 as $2^4 = 5$ modulo 11.

There is no known polynomial time algorithm for computing the discrete logarithm of $a$ modulo $p$ to the base $r$ (when given the prime $p$, a root $r$ modulo $p$, and a positive integer $a \in \mathbf{Z}_p$). The problem plays a role in cryptography as will be discussed in Section 4.6.