Discrete Structures

Spring 2020

Number Theory

Text book: Kenneth H. Rosen, Discrete Mathematics and Its Applications

Section: 4.3 and 4.4

Primes and Greatest Common Divisors

Section 4.3

Primes

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*.

Example: The integer 7 is prime because its only positive factors are 1 and 7, but 9 is composite because it is divisible by 3.

The Fundamental Theorem of Arithmetic

Theorem: 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.

Examples:

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

Erastothenes
(276-194 B.C.)

The Sieve of Erastosthenes (page 259)

- The *Sieve of Erastosthenes* can be used to find all primes not exceeding a specified positive integer. For example, begin with the list of integers between 1 and 100.
  a. Delete all the integers, other than 2, divisible by 2.
  b. Delete all the integers, other than 3, divisible by 3.
  c. Next, delete all the integers, other than 5, divisible by 5.
  d. Next, delete all the integers, other than 7, divisible by 7.
  e. Since all the remaining integers are not divisible by any of the previous integers, other than 1, the primes are:

{2,3,5,7,11,13, 17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89, 97}

continued →

The Sieve of Erastosthenes

TABLE 1 **The Sieve of Eratosthenes.**

Integers divisible by 2 other than 2 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 3 other than 3 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 5 other than 5 receive an underline.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Integers divisible by 7 other than 7 receive an underline; integers in color are prime.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

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

To see this, note that if $n = ab$, then $a \le \sqrt{n}$ or $b \le \sqrt{n}$.

Trial division, a very inefficient method of determining if a number n is prime, is to try every integer $i \le \sqrt{n}$ and see if n is divisible by i.

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.

Example

- Find the prime factorization of 1111 and 909090
- Solution:
- $1111 = 11 \cdot 101$
- $909090 = 2 \cdot 454545 = 2 \cdot 3 \cdot 151515 = 2 \cdot 3 \cdot 3 \cdot 50505$

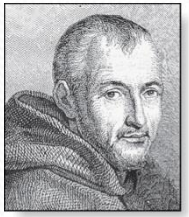
  $= 2 \cdot 3 \cdot 3 \cdot 3 \cdot 16835 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 3367 = 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 7 \cdot 481$

  $= 2 . 3 . 3 . 3 . 5 . 7 . 13 . 37 = 2 . 3^3 . 5 . 7 . 13 . 37$

Infinitude of Primes

Euclid
(325 B.C.E. – 265 B.C.E.)

Theorem: There are infinitely many primes. (Euclid)



Marin Mersenne
(1588-1648)

Mersenne Primes (page 261)

Definition: Prime numbers of the form $2^p - 1$, where p is prime, are called *Mersenne primes*.

- $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 37$, and $2^7 - 1 = 127$ are Mersenne primes.
- $2^{11} - 1 = 2047$ is not a Mersenne prime since $2047 = 23 \cdot 89$.
- There is an efficient test for determining if $2^p - 1$ is prime.
- The largest known prime numbers are Mersenne primes.
- As of mid 2014, 48 Mersenne primes were known, the largest is $2^{57,885,161} - 1$, which has nearly 17 million decimal digits.
- The *Great Internet Mersenne Prime Search* (*GIMPS*) is a distributed computing project to search for new Mersenne Primes.

Distribution of Primes (page 262)

- Mathematicians have been interested in the distribution of prime numbers among the positive integers. In the nineteenth century, the *prime number theorem* was proved which gives an asymptotic estimate for the number of primes not exceeding x.

  Prime Number Theorem: The ratio of the number of primes not exceeding x and $x/\ln x$ approaches 1 as x grows without bound. ($\ln x$ is the natural logarithm of x)
  - The theorem tells us that the number of primes not exceeding x, can be approximated by $x/\ln x$.
  - The odds that a randomly selected positive integer less than n is prime are approximately $(n/\ln n)/n = 1/\ln n$.

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. 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: gcd(24,36) = 12

Example:What is the greatest common divisor of 17 and 22?

Solution: gcd(17,22) = 1

Greatest Common Divisor

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

Example: 17 and 22 are relatively prime because gcd(17, 22)=1.

Definition: 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.

Solution: Because gcd(10,17) = 1, gcd(10,21) = 1, and gcd(17,21) = 1, 10, 17, and 21 are pairwise relatively prime.

Example: Determine whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution: Because gcd(10,24) = 2>1, so 10, 19, and 24 are not pairwise relatively prime.

Finding the Greatest Common Divisor Using Prime Factorizations

- Suppose the prime factorizations of *a* and *b* are:

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

where each exponent is a nonnegative integer, and where all primes occurring in either prime factorization are included in both. Then:

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

- This formula is valid since the integer on the right (of the equals sign) divides both *a* and *b*. No larger integer can divide both *a* and *b*.

Example: $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$

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

- Finding the gcd of two positive integers using their prime factorizations is not efficient because there is no efficient algorithm for finding the prime factorization of a positive integer.

Least Common Multiple

Definition: The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b. It is denoted by $\text{lcm}(a,b)$.

- The least common multiple can also be computed from the prime factorizations.

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

This number is divided by both a and b and no smaller number is divided by a and b.

Example: $\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^4\, 3^5\, 7^2$

- The greatest common divisor and the least common multiple of two integers are related by:

Theorem 5: Let a and b be positive integers. Then

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

(*proof is Exercise* 31)

Euclidean Algorithm

Euclid
(325 B.C.E. – 265 B.C.E.)

- The Euclidian algorithm is an efficient method for computing the greatest common divisor of two integers. It is based on the idea that gcd(a,b) is equal to gcd(b,r) when $a > b$ and r is the remainder when a is divided by b.

Example: Find gcd(91, 287):

- $287 = 91 \cdot 3 + 14$ Divide 287 by 91
- $91 = 14 \cdot 6 + 7$ Divide 91 by 14
- $14 = 7 \cdot 2 + 0$ Divide 14 by 7

Stopping condition

gcd(287, 91) = gcd(91, 14) = gcd(14, 7) = 7

continued →

Euclidean Algorithm

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 $a - bq = r$ (by Theorem 1 of Section 4.1). 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 a and b must also be a common divisor of b and r.
- Therefore, $\gcd(a,b) = \gcd(b,r)$. ◀

Euclidean Algorithm

- Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. Successive applications of the division algorithm yields:

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 \leq r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3 && 0 \leq r_3 < r_2, \\
&\ \ \vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 \leq r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n .
\end{aligned}
$$

- Eventually, a remainder of zero occurs in the sequence of terms: $a = r_0 > r_1 > r_2 > \cdots \geq 0$. The sequence can't contain more than a terms.
- By result on previous slide

  $\gcd(a,b) = \gcd(r_0,r_1) = \cdots = \gcd(r_{n-1},r_n) = \gcd(r_n, 0) = r_n$.
- Hence the greatest common divisor is the last nonzero remainder in the sequence of divisions.

Étienne Bézout
(1730-1783)

gcds as Linear Combinations

Bézout's Theorem: If a and b are positive integers, then there exist integers s and t such that $\gcd(a,b) = sa + tb$.

Definition: If a and b are positive integers, then integers s and t such that $\gcd(a,b) = sa + tb$ are called *Bézout coefficients* of a and b. The equation $\gcd(a,b) = sa + tb$ is called *Bézout's identity*.

- By Bézout's Theorem, the gcd of integers a and b can be expressed in the form $sa + tb$ where s and t are integers. This is a *linear combination* with integer coefficients of a and b.
  - $\gcd(6,14) = (-2)\cdot 6 + 1\cdot 14$

Finding gcds as Linear Combinations

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

Solution: First use the Euclidean algorithm to show gcd(252,198) = 18

i. $252 = 1 \cdot 198 + 54$
ii. $198 = 3 \cdot 54 + 36$
iii. $54 = 1 \cdot 36 + 18$
iv. $36 = 2 \cdot 18$

- Now working backwards, from iii and i above
  - $18 = 54 - 1 \cdot 36$
  - $36 = 198 - 3 \cdot 54$
- Substituting the 2nd equation into the 1st yields:
  - $18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$
- Substituting $54 = 252 - 1 \cdot 198$ (from i)) yields:
  - $18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$

continued →

Finding gcds as Linear Combinations

- This method illustrated above is a two pass method. It first uses the Euclidian algorithm to find the gcd and then works backwards to express the gcd as a linear combination of the original two integers. A one pass method, called the *extended Euclidean algorithm*, is developed in the exercises.

Consequences of Bézout's Theorem

Lemma 2: If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof: Assume $\gcd(a, b) = 1$ and $a \mid bc$

- Since $\gcd(a, b) = 1$, by Bézout's Theorem there are integers s and t such that

$$sa + tb = 1.$$

- Multiplying both sides of the equation by c, yields $sac + tbc = c$.
- From Theorem 1 of Section 4.1:

  $a \mid tbc$ (part ii) and a divides $sac + tbc$ since $a \mid sac$ and $a \mid tbc$ (part i)
- We conclude $a \mid c$, since $sac + tbc = c$. ◀

Consequences of Bézout's Theorem

Lemma 3: If p is prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_i$ for some i.

- Lemma 3 is crucial in the proof of the uniqueness of prime factorizations.

Uniqueness of Prime Factorization

(page 271)

- A prime factorization of a positive integer where the primes are in nondecreasing order is unique.

Dividing Congruences by an Integer

- Dividing both sides of a valid congruence by an integer does not always produce a valid congruence (see Section 4.1).
- But dividing by an integer relatively prime to the modulus does produce a valid congruence:

Theorem 7: Let m be a positive integer and let *a, b,* and *c* be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c,m) = 1$, then $a \equiv b \pmod{m}$.

Proof: Since $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$ by Lemma 2 and the fact that $\gcd(c,m) = 1$, it follows that $m \mid a - b$. Hence, $a \equiv b \pmod{m}$. ◀

Exercise (Q.6.)

How many zeros are there at the end of 100!?

There are plenty of factors 2 in 100!, so the question is how many factors 5 are there?

100! has $\frac{100}{5}$=20 terms divisible by 5^1,
namely 5,10,15,20,...,100

It has $\frac{100}{25}$=4 terms divisible by 5^2 , namely 25,50,75,100.

So there are a total of 20+4=24 factors 5 in 100!.

Hence 100! is divisible by 1024 and no greater power of 10.
So 100! ends with 24 zeros.

Exercise (Q.39.) express the greatest common divisor of each of these pairs of integers as a linear combination of these integers____________ (i)9999, 11111

Euclidean algorithm

11111=9999+1112

9999 = 8 . 1112 + 1103

1112 = 1103 + 9

1103 = 122 . 9 + 5

9=5+4

5=4+1

Backward substitution

1=5-4

= 5 - (9 - 5) = 2 . 5 - 9

= 2 . (1103 - 122 . 9) – 9

= 2 . 1103 - 245 . 9

= 2. 1103 - 245. (1112 - 1103)

= 247. 1103 - 245. 1112

= 247. (9999 - 8. 1112) - 245. 1112

= 247. 9999 - 2221 . 1112

= 247. 9999 - 2221. (11111 - 9999)

= 2468. 9999 - 2221. 11111

Solving Congruences

Section 4.4

Linear Congruences

Definition: A congruence of the form

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

where m is a positive integer, a and b are integers, and x is a variable, is called a *linear congruence*.

- The solutions to a linear congruence $ax \equiv b(\bmod m)$ are all integers x that satisfy the congruence.

Definition: An integer $\bar{a}$ such that $\bar{a}a \equiv 1(\bmod m)$ is said to be an *inverse* of a modulo m.

Example: 5 is an inverse of 3 modulo 7 since $5 \cdot 3 = 15 \equiv 1(\bmod 7)$

- One method of solving linear congruences makes use of an 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

- The following theorem guarantees that an inverse of a modulo m exists whenever a and m are relatively prime. Two integers a and b are relatively prime when $\gcd(a,b) = 1$.

  Theorem : If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m. (This means that there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.)

  Proof: Since $\gcd(a,m) = 1$, by Theorem 6 of Section 4.3, there are integers s and t such that $sa + tm = 1$.

  - 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.

◀

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 on previous slide , an inverse of 3 modulo 7 exists.

  - Using the Euclidian algorithm: $7 = 2\cdot 3 + 1$.
  - From this equation, we get $-2\cdot 3 + 1\cdot 7 = 1$, and see that -2 and 1 are Bézout coefficients of 3 and 7.
  - Hence, -2 is an inverse of 3 modulo 7.
  - Also every integer congruent to -2 modulo 7 is an inverse of 3 modulo 7, i.e., 5, -9, 12, etc.

Finding Inverses

Example: Find an inverse of 101 modulo 4620.

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

Working Backwards:

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

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

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

Bézout coefficients : − 35 and 1601

1601 is an inverse of 101 modulo 4620

Using Inverses to Solve Congruences

- We can solve the congruence $ax \equiv b(\bmod m)$ by multiplying both sides by $\bar{a}$.

  Example: What are the solutions of the congruence $3x \equiv 4(\bmod 7)$.

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

  $$-2 \cdot 3x \equiv -2 \cdot 4 (\bmod 7).$$

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

  We need to determine if every x with $x \equiv 6 \pmod 7$ is a solution. Assume that $x \equiv 6 \pmod 7$. By Theorem 5 of Section 4.1, it follows that $3x \equiv 3 \cdot 6 = 18 \equiv 4(\bmod 7)$ which shows that all such x satisfy the congruence.

  The solutions are the integers x such that $x \equiv 6 \pmod 7$, namely, $6, 13, 20 \ldots$ and $-1, -8, -15, \ldots$

The Chinese Remainder Theorem

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

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

- This puzzle can be translated into the solution of the system of congruences:

  $x \equiv 2 \pmod{3}$,

  $x \equiv 3 \pmod{5}$,

  $x \equiv 2 \pmod{7}$?

- We'll see how the theorem that is known as the *Chinese Remainder Theorem* can be used to solve Sun-Tsu's problem.

The Chinese Remainder Theorem

Theorem 2: (*The Chinese Remainder 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

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\vdots \\
x &\equiv a_n \pmod{m_n}
\end{aligned}
$$

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

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

- **Proof**: We'll show that a solution exists by describing a way to construct the solution. Showing that the solution is unique modulo m 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 Theorem 1, there is an integer y_k, an inverse of M_k modulo m_k, such that

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

Form the sum

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

Note that because $M_j \equiv 0 \pmod{m_k}$ whenever $j \neq k$, all terms except the kth term in this sum are congruent to 0 modulo 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.

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

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

  Example: Use the method of back substitution to find all integers x such that $x \equiv 1 \pmod{5}$, $x \equiv 2 \pmod{6}$, and $x \equiv 3 \pmod{7}$.

Back Substitution

- **Solution**: By Theorem 4 in Section 4.1, the first congruence can be rewritten as $x = 5t + 1$, where t is an integer.
  - 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 the solution $x \equiv 206 \pmod{210}$.

Fermat's Little Theorem

Pierre de Fermat
(1601-1665)

Theorem 3: (*Fermat's Little Theorem*) If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$
Furthermore, for every integer a we have $a^p \equiv a \pmod{p}$
(*proof outlined in Exercise 19*)

Fermat's little theorem is useful in computing the remainders modulo p of large powers of integers.

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

By Fermat's little theorem, we know that $7^{10} \equiv 1 \pmod{11}$, and so $(7^{10})^k \equiv 1 \pmod{11}$, for every positive integer k. Therefore,

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

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