4.2

Modular Exponentiation:

- Allows you to get the remainder of dividends with large exponents.

Steps

- Convert exponent to binary.
- Take number of binary digits, and that will be the number of modular exponentiation steps needed
- Starting with the base to the power of 1 (i.e. $base^1$ mod d), calculate its result
- Do that for all steps but continuously double the exponent.
- once done, for each step associated to a binary digit value of 1, multiply each corresponding modulus result and then mod it by the divisor.

Rules

$a \cdot b \cdot c \bmod x = [(a \cdot b \bmod x) \cdot (c \bmod x)] \bmod x$

$a \bmod b = (a \bmod b) \bmod b$

ex: $3^{50} \bmod 16 = ?$

Solution:

- convert 50 to binary.

$2 \overline{)50}$ 25 r 0

$2 \overline{)25}$ 12 r 1

$2 \overline{)12}$ 6 r 0

$2 \overline{)3}$ 1 r 1

$2 \overline{)1}$ 0 r 1

$(50)_{10} = (110010)_2$

$50 = 2^5 + 2^4 + 2^1$

$= 32 + 16 + 2$

$3^{50} = 3^{32} \cdot 3^{16} \cdot 3^2$

$3^{50} \bmod 16 = [(3^{32} \bmod 16) \cdot (3^{16} \bmod 16) \cdot (3^{2} \bmod 16)] \bmod 16$

$(1\,1\,0\,0\,1\,0)_2$ ← 6 digits = 6 modular exponentiation steps.

6 5 4 3 2 1

step #	Modular Exponentiation
1	$3^1 \bmod 16 = 3$
2	$3^2 \bmod 16 = 9$
3	$3^4 \bmod 16 = 81 \bmod 16 = 1$
4	$3^8 \bmod 16 = 3^4 \cdot 3^4 \bmod 16 = 1 \cdot 1 \bmod 16 = 1$
5	$3^{16} \bmod 16 = 3^8 \cdot 3^8 \bmod 16 = 1 \cdot 1 \bmod 16 = 1$
6	$3^{32} \bmod 16 = 3^{16} \cdot 3^{16} \bmod 16 = 1 \cdot 1 \bmod 16 = 1$

$3^{50} \bmod 16 = (9 \cdot 1 \cdot 1) \bmod 16 = \boxed{9}$

$(a \cdot b \cdot c \cdot d) \bmod x$

$[(a \cdot b \bmod x) \cdot (c \cdot d \bmod x)] \bmod x$

Section 4.3 - Primes and Greatest Common Divisors

- An integer p greater than 1 is called prime if the only positive factors of p are 1 and p.
- A positive integer greater than 1 and not prime is called composite.
  - i.e. An integer n is composite if and only if there exists an integer a such that $a|n$ and $1 < a < n$.
- 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.
- Theorem 2: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

ex: Is 101 prime?

Solution:

$\sqrt{101} \approx 10.05$

2, 3, 5, 7 do not divide 101. Therefore 101 is prime.

ex: Find the prime factorization of 100

Solution:

$\begin{array}{r} 50 \\ 2\overline{)100} \end{array}$ $\quad$ $\begin{array}{r} 5 \\ 5\overline{)25} \end{array}$ $\quad$ $100 = 2 \cdot 2 \cdot 5 \cdot 5$

$\begin{array}{r} 25 \\ 2\overline{)50} \end{array}$ $\quad$ $5\overline{)5}$ $\quad$ $100 = \boxed{2^2 \cdot 5^2}$

$2 \nmid 25$

$3 \nmid 25$

ex: Find the prime factorization of 7007.

Solution

$\sqrt{7007} \approx 83.7$

If no prime from 2 to 83 divides 7007, then 7007 is prime.

$2 \nmid 7007$

$3 \nmid 7007$

$5 \nmid 7007$

$7 \mid 7007$ ← this tells us 7007 is not prime

$\begin{array}{r} 1001 \\ 7\overline{)7007} \end{array}$

no need to check for 2, 3, 5 divides 1001, because those do not divide 7007.

$\begin{array}{r} 143 \\ 7\overline{)1001} \end{array}$ $\quad$ $\begin{array}{r} 13 \\ 11\overline{)143} \end{array}$

$7 \nmid 143$ $\quad$ $\begin{array}{r} 1 \\ 13\overline{)13} \end{array}$ ← stop once quotient is 1.

$11 \mid 143$

$7007 = 7 \cdot 7 \cdot 11 \cdot 13$

$= \boxed{7^2 \cdot 11 \cdot 13}$

GCD

Definition 2: Let a and b be integers, both nonzero. The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor.

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

ex: What's the gcd of 100 and 7007?

$7007 = 7 \cdot 7 \cdot 11 \cdot 13$
$100 = 2^2 \cdot 5^2$

Solution: Find prime factorization of 100 and 7007

$7007 = 7^2 \cdot 11 \cdot 13$

$100 = 2^2 \cdot 5^2$

$$\gcd(100, 7007) = 2^{\min(2,0)} 5^{\min(2,0)} 7^{\min(0,2)} 11^{\min(0,1)} 13^{\min(0,1)}$$

$$= 2^0 \cdot 5^0 \cdot 7^0 \cdot 11^0 \cdot 13^0 = \boxed{1}$$

Definition 3: The integers a and b are relatively prime if their gcd is 1.

Definition 4: The integers $a_1, a_2, \dots, a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i \leq j \leq n$

a, b, c are integers

if $\gcd(a,b) = 1$

$\gcd(a,c) = 1$

$\gcd(b,c) = 1$

Then a, b, and c are pairwise relatively prime.

ex: Find the gcd of 24 and 36.

Solution:

Prime factorization of 24:

$$2\,\overline{)24}^{\,12}$$
$$2\,\overline{)12}^{\,6}$$
$$2\,\overline{)6}^{\,3}$$
$$3\,\overline{)3}^{\,1}$$

$24 = 2\cdot 2\cdot 2\cdot 3$

$= 2^3\cdot 3$

Prime Factorization of 36:

$$\begin{array}{ccccccc} & & & 36 & & & \\ & & 4 & & 9 & & \\ & 2 & 2 & & 3 & 3 & \end{array}$$

$= 2^2\cdot 3^2$

$\gcd(24,36) = 2^{\min(3,2)}\cdot 3^{\min(1,2)}$

$= 2^2\cdot 3 = \boxed{12}$

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.

- Denoted $\mathrm{lcm}(a,b)$

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

ex: Find $\mathrm{lcm}(24,36)$

Solution:

$24 = 2^3\cdot 3$

$36 = 2^2\cdot 3^2$

$\mathrm{lcm}(24,36) = 2^{\max(3,2)}\, 3^{\max(1,2)} = 2^3\cdot 3^2 = 8\cdot 9 = \boxed{72}$