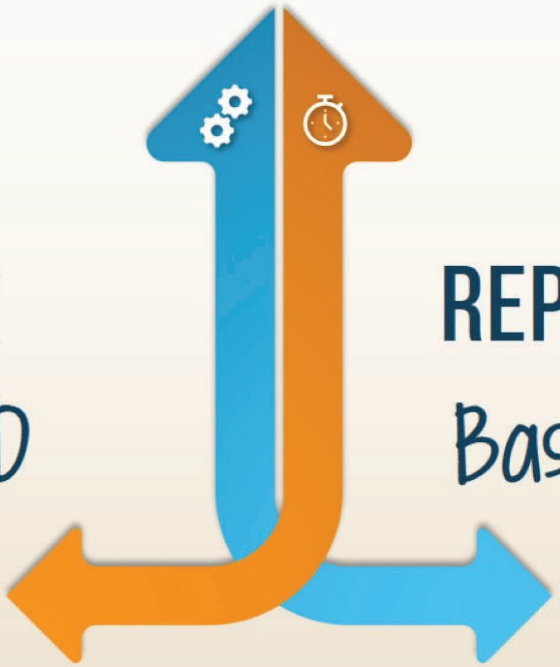
PROPERTIES OF INTEGERS

EUCLIDEAN ALGORITHM

Finding GCD



INTEGER REPRESENTATION

Base Conversion

Learning objectives! Know what you will learn today

Self-Reflection! Rate levels of your understanding

❍ Checklist of key topics. Keep catching up with the course.

- ☐ Find GCD using the Euclidean algorithm
- ☐ Find s and t using the extended Euclidean algorithm
- ☐ Understand values and representations of integers
- ☐ Conversion between decimal numbers and other bases
- ☐ Conversion between certain bases using grouping of digits

Confident	Got it	Okay	Fuzzy	Not a clue

GCD (47376,78255) = ?

Factoring ?

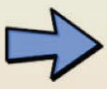
Make the numbers smaller and find GCD of smaller pairs ...

- $a = kb + r$ — Given a & b we can find k & r
- GCD (a, b) = GCD (b, r) — Integers b & r are smaller than a & b

Euclidean algorithm – To compute the GCD of a and b, recursively find k and r such that a = kb + r and compute the GCD of b and r.

Use Euclidean Algorithm to Compute GCD(273,98)

Iteration	a	b	r	a = kb + r



GCD(273,98) = ?

Use Euclidean Algorithm to Compute GCD(273,98)

a = kb + r

- From running the Euclid's algorithm, we got the GCD of **not one but multiple pairs** of integers

Extended Euclidean Algorithm

- Used to find two integers s and t (not necessarily positive) such that

$$GCD(a, b) = d = sa + tb$$

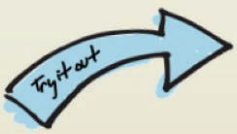
You are not responsible for a proof of this theorem but ***you must be able to compute the GCD and integers s and t.***

Use Extended Euclid to find s,t in 7 = s × 273 + t × 98

a = kb + r

Extended Euclidean Algorithm GCD (a, b) = d = sa + tb

- Find integers x and y such that $z = xa + yb$
- If $z = \text{GCD}(a,b)$, then x and y are s and t, by the extended Euclid's alg.
- If z is not equal to the GCD of a and b, then we need one extra step



❑ Find x and y such that $(x)(273) + (y)(98) = 70$

http://mathforum.org/library/drmath/view/51595.html

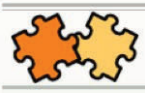
PRACTICE PROBLEMS

Let a=108 and b=60, find d=GCD(a,b) and find s,t such that d=sa+tb
Determine whether there exist $(x, y) \in \mathbb{Z}$ such that $108x + 60y = 40$

PRACTICE PROBLEMS

Find the greatest common divisor d of a and b and write d as sa+tb

- a = 45 and b = 33



PRACTICE PROBLEMS

Find the greatest common divisor d of a and b and write d as sa+tb

- a = 77 and b = 128

PRACTICE PROBLEMS

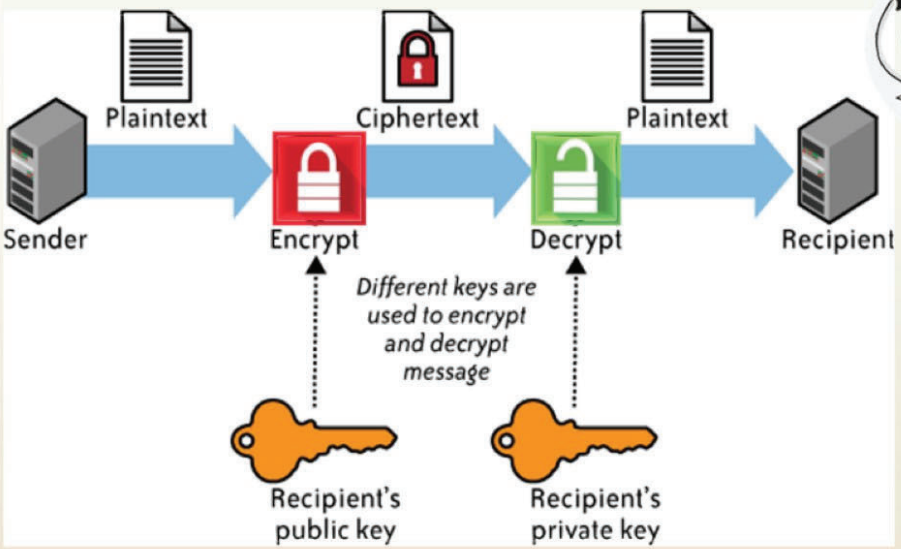
Given integers: a = 7854 and b = 4746, find x and y such that xa + yb = GCD(a,b) and then determine the least common multiple of a and b

What will be on the quiz?

- Use Euclidean and the extended algorithms to compute GCD(a,b) and s and t. Fill in the values of a & b at each iteration
- … with a couple of follow-up questions

Iteration	a	b
1	?	?
2	?	?
3	?	?
4	?	?

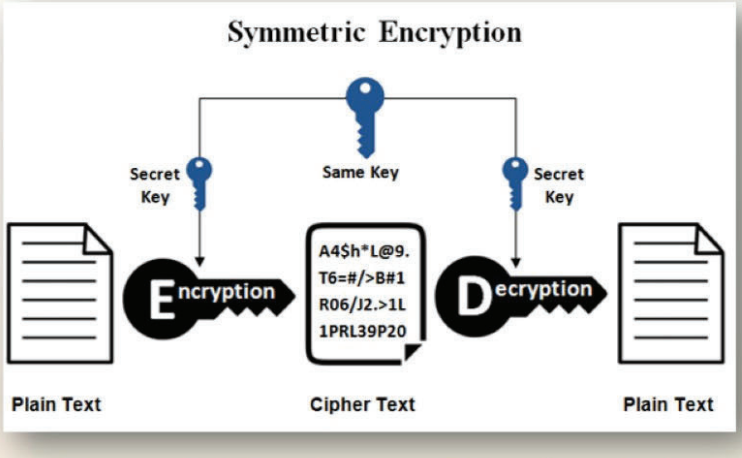
What are applications of extended Euclidean alg?

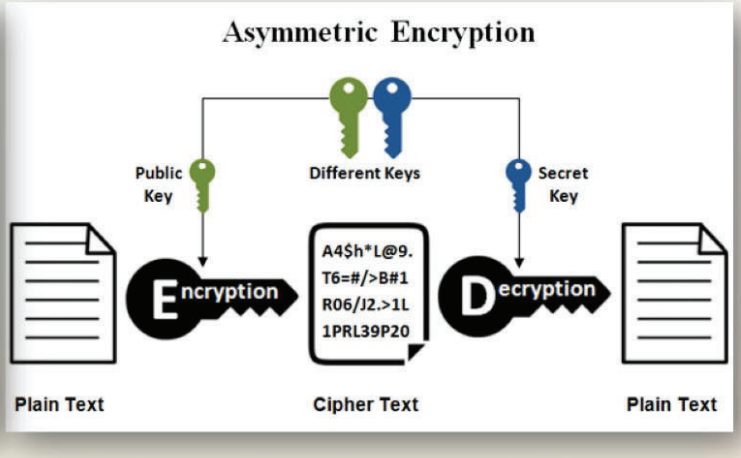


https://shankaraman.wordpress.com/tag/creating-public-and-private-key-using-gpg/

Why we need s and t ?

GCD(a,b) = d = sa + tb Why do we need to calculate it? What is it for?





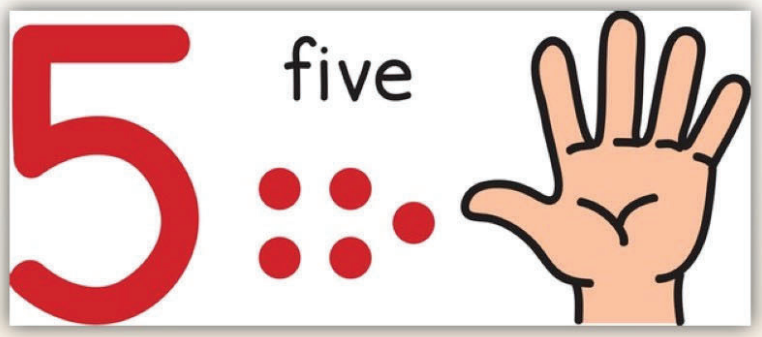
Caesar Cipher is one of the simplest symmetric encryption techniques

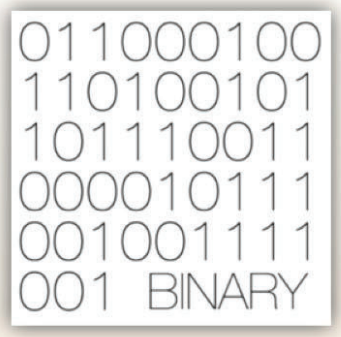
Public-private keys are different but mathematically linked

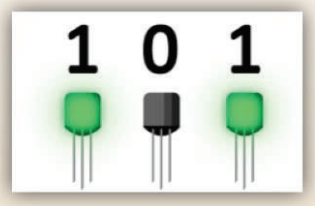
REPRESENTATIONS OF INTEGERS

Properties of Integers

Counting to "five"... Representing the value "five"...





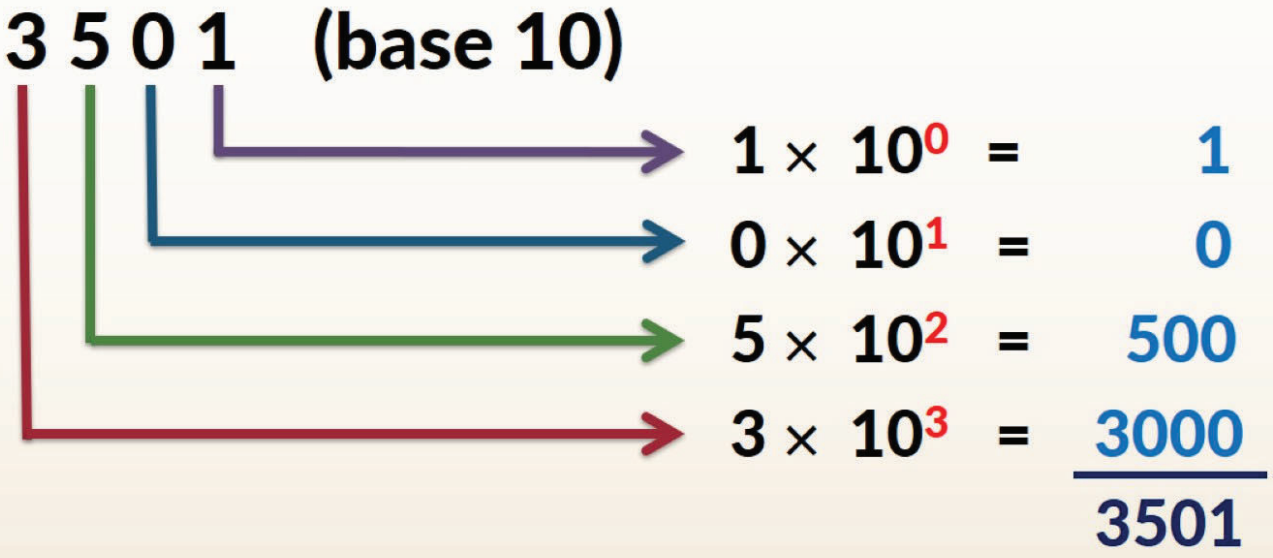


To represent any number, no matter how large or how small

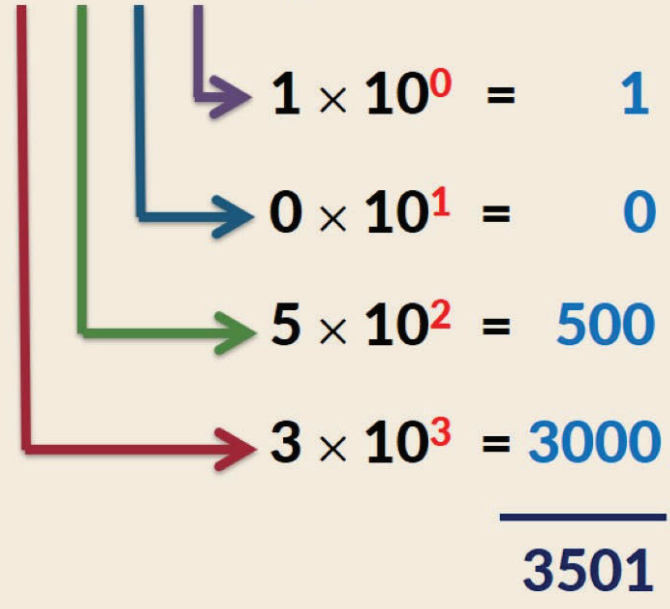
Numbering Systems	Base	Digits
Binary	2	0, 1
Octal	8	0, 1, 2, 3, 4, 5, 6, 7
Decimal	10	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Hexadecimal	16	0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F

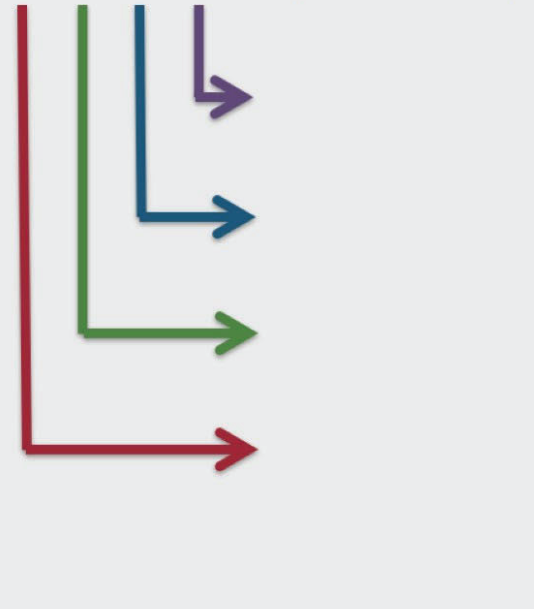
These are common bases in digital technology; in general, base $b \in \mathbb{Z}^+$

- Know how to **count** and how to **convert** from one base to another
- Know how to **add**, **subtract**, **multiply**, and **divide** in different bases
- Know how to encode & decode messages using base 26 **Bacon's code**

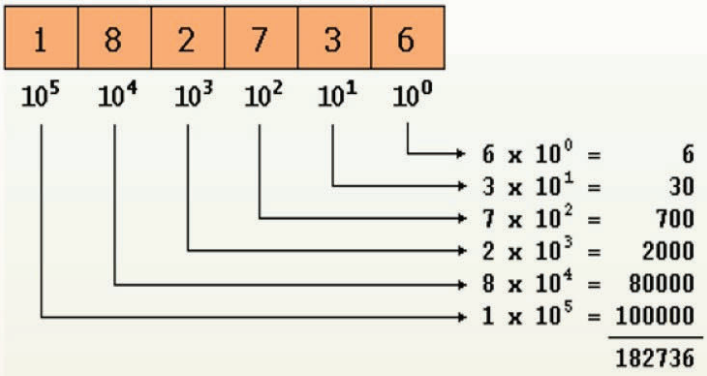


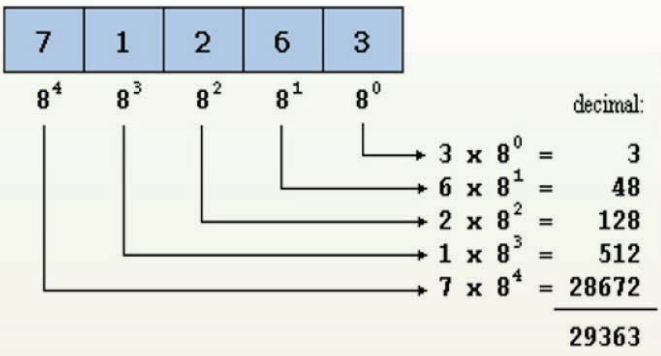
- Each position to the left of the decimal point has the **base value** equal to **the base raised to the power of the position** where the first position is zero. In decimal, this is $10^0=1$; $10^1=10$; $10^2=100$.



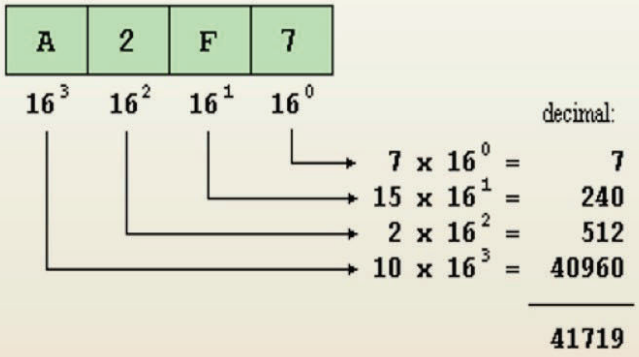


Conversion from any base b to base 10





- Base 8 has 8 digits: 0–7
- Base 10 has 10 digits: 0–9
- Base 16 has 16 digits: 0–9 , A–F
- A base can be any integer b > 0

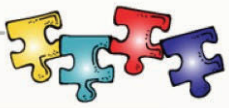


http://www.cplusplus.com/doc/hex/

WORKED EXAMPLES

- Convert a binary number 111000 to decimal

WORKED EXAMPLES



- Convert 0x5D5E to decimal number
  - Notation: when writing a hexadecimal number (base 16), it is preceded with 0x. That is, $0x5D5E = 5D5E_{16}$

Convert 432 base 10 to base 5

- Repeatedly divide 432 by 5 until the quotient is less than the divisor.
- The result is the remainder read from the bottom up.

Conversion from base 10 to any base b

WORKED EXAMPLES

- Convert a decimal number 23902 to base 18

What have we learned so far?

- Convert from any base b1 to base 10 – by **power expansion**
- Convert from base 10 to any base b2 – by **repeated division**

⇨Therefore, through base 10, we can convert from any base b1 to b2

Convert the number 5D5E base 16 to base 18

Step1: convert base 16 to base 10

Conversion between bases other than base 10

Step2: convert base 10 to base 18

Note: we did both of these conversions in the previous worked examples

WORKED EXAMPLES

- Convert the number 4067 base 23 to hexadecimal

Step1: convert base 23 to base 10

Step2: convert base 10 to base 16

PRACTICE PROBLEMS

- Convert the number A5BC base 13 to base 6

Step1: convert base 13 to base 10

Step2: convert base 10 to base 6

PRACTICE PROBLEMS

- Convert the following numbers to base 10

I. $(100110101)_2$ II. $(666421)_7$ III. $(1GA5)_{17}$

PRACTICE PROBLEMS

- Convert the following decimal numbers to the bases stated.

I. 55 to binary

II. 56789 to base 9

III. 493314 to base 14

PRACTICE PROBLEMS

Perform the following base conversions

I. **4** base 6 to base 20

II. **D** base 14 to base 13

III. **3207** octal to base 12

PRACTICE PROBLEMS

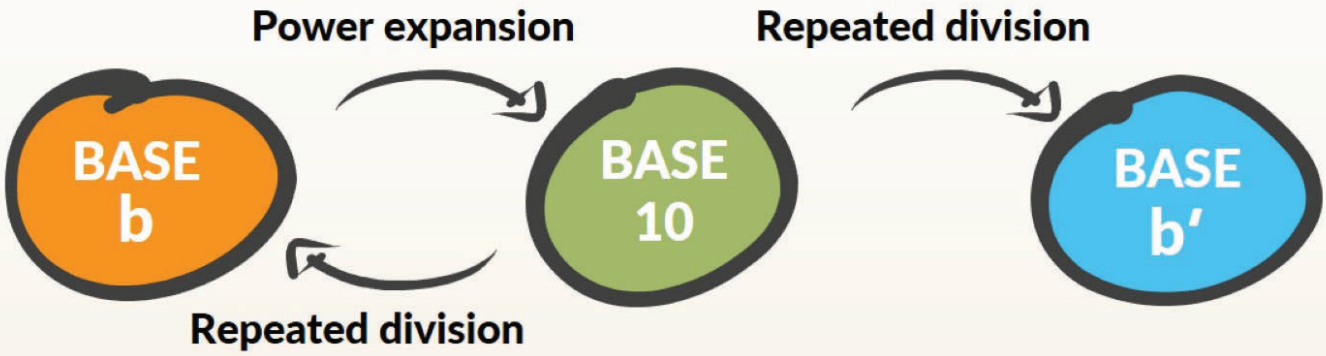
Perform the following base conversions

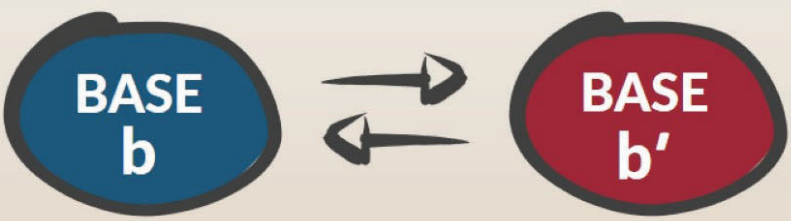
IV. **0xAF4** to base 7

V. **3210** base 5 to base 3

VI. **212** base 3 to base 5

Conversion between any bases





A one-step conversion between non-decimal number bases b and b'

Base conversion trick by grouping of digits

- This is related to factorization and the distributive law Base 2 to 4

$$100111_2 = 1\times2^5 + 0\times2^4 + 0\times2^3 + 1\times2^2 + 1\times2^1 + 1\times2^0$$

Base conversion trick by grouping of digits

- This is related to factorization and the distributive law Base 2 to 8

$$100111_2 = 1\times2^5 + 0\times2^4 + 0\times2^3 + 1\times2^2 + 1\times2^1 + 1\times2^0$$

Conversion without converting to decimal numbers

- To convert from base 2 (binary) numbers to base 8 (octal) numbers,
  - **group binary digits into groups of 3 bits**, start grouping from the ***least significant bit***. Then, **write each group in octal digit**.

$$1\ 100\ 101\ 011\ 111_2 \Rightarrow$$

- From octal to binary, **encode each octal digit using 3-bits binary**

$$62510_8 \Rightarrow$$

Base conversion trick by grouping of digits

- Between **binary** & base **4** → group binary digits into group of _____
  - We need **2** binary-bits to write the digits 0,1,2,3 of base 4 → $2^2 = 4$
- Between **binary** & base **8** → group binary digits into group of _____
  - We need **3** binary-bits to write the digits 0,1,2,3,4,5,6,7 of base 8 → $2^3 = 8$
- Between **binary** & base **16** → group binary digits into group of _____
  - We need **4** binary-bits to write the digits 0,1,2,3,…,14,15 of base 16 → $2^4 = 16$

From smaller to larger base -> go from n digits to 1 digit
From larger to smaller base -> expand each digit to n digits

Base conversion trick by grouping of digits

- In the following, if the trick applies, how many digits are grouped?

  Base 3 and 9

  Base 3 and 27

  Base 4 and 8

  Base 4 and 16

Between which other bases would this conversion trick apply?

This works when the larger base is some power of a smaller base.

WORKED EXAMPLES

- Convert 123103312 in base 4 to hexadecimal

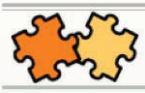
WORKED EXAMPLES

- Convert $(K9)_{27}$ to base 3

PRACTICE PROBLEMS

- Convert $(1101\ 0101\ 1100\ 1111)_2$ to base 4, octal, and hexadecimal

- Convert $(1AB8D94E)_{16}$ to binary, base 4, and octal number



PRACTICE PROBLEMS

- Convert $(4353)_8$ to base 4, base 16, and base 64
  For base64, use alphabets: 012…789ABCD…XYZabc…xyz+=

- Convert $(111)_6$ to base 3 and base 36

PRACTICE PROBLEMS

Convert the following to base 5.

- 25050 base 10

- DANCE base 25

- ZEBRA base 50

PRACTICE PROBLEMS

- Determine which of the following numbers are multiples of five. Select all that are true. Hint: think divisibility and power expansion, a full conversion to decimal numbers is not needed.

- ☐ $(117)_9$
- ☐ $(111100)_2$
- ☐ $(4105)_6$
- ☐ $(A1BA)_{15}$

What's next?