3 is the mult inv of 2 mod 5

$2 \cdot 3 \bmod 5 = 1$

Note Title 10/29/2014

Let $n$ be an integer $> 1$.

$a, b \in \mathbb{Z}_n$ $\quad a, b \in \{0, \dots, n-1\}$.

$a$ is multiplicative inverse of $b$ mod $n$ if

$$a \cdot b \equiv 1 \bmod n. = (a \cdot b \bmod n = 1)$$

A multiplicative inverse does not always exist.

4 does not have a multiplicative inverse mod 6.

$$\nexists x \quad x \cdot 4 \equiv 1 \bmod 6$$

Fact: "a" has a multiplicative inverse mod $n$ if and only if $a$ & $n$ are relatively prime $(\gcd(a,n) = 1)$.

Will show one direction for this:

$$\gcd(a,n) = 1.$$

$\exists$ integers $s, t$. $\quad s \cdot a + \underbrace{t \cdot n}_{} \overset{0}{=} 1.$

$$\underline{s} \cdot a \equiv 1 \bmod n.$$

$$\underbrace{(s \bmod n)}_{\text{multiplicative inverse.}} \cdot a \bmod n = 1$$

Find the multiplicative inverse of 9 mod 32.

$32 \quad 9 \quad 5 \quad 4 \quad 1$

$s \cdot 9 + 32 \cdot t = 1$

$1 = 5 - 4$ ①

$4 = 9 - 5$ ②

$5 = 32 - 3 \cdot 9$ ③

(32 div 9)

$$\begin{aligned} 1 &= 5 - 4 \\ &= 5 - (9 - 5) \\ &= -1 \cdot 9 + 2 \cdot 5 \\ &= -1 \cdot 9 + 2(32 - 3 \cdot 9) \\ &= 2 \cdot 32 - 7 \cdot 9 \end{aligned}$$

$(-7) \cdot 9 + 2 \cdot 32 = 1$

mult inv $=$ $(-7 \bmod 32 = 25)$

$(25 \cdot 9) \equiv 1 \bmod 32.$

Find the mult inv. of 28 mod 135

# 8.4 Number Representation.

Numbers in decimal notation:

Sequence of digits $\{0, 1, 2, \ldots, 9\}$

$$314 = 3\cdot 100 + 1\cdot 10 + 4$$
$$= 3\cdot 10^2 + 1\cdot 10^1 + 4\cdot 10^0$$

Computers represent numbers in binary:

$$(101101)_2 = 1\cdot 2^5 + \cancel{0\cdot 2^4} + \cancel{1\cdot 2^3} + 1\cdot 2^2 + \cancel{0\cdot 2^1} + 1\cdot 2^0$$
$$= 32 + 8 + 4 + 1 = 45$$

**Theorem** For any integer $b > 1$, every non-negative integer $n$ can be expressed uniquely as:

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 \cdot b^1 + a_0 b^0$$

$a_k > 0$ for $j = 0, \ldots, k$ $a_k \in \underbrace{\{0, \ldots, b-1\}}_{\text{digits base } b}$.

base $b$ representation of $n$: (expansion)

$$n = (a_k a_{k-1} \cdots a_2 a_1 a_0)_b$$

Converting base b into decimal:

$(3011)_4 = 3 \cdot 4^3 + 0 \cdot 4^2 + 1 \cdot 4^1 + 1 \cdot 4^0$

$= 3 \cdot 64 + 4 + 1 = \underline{\underline{197}}$

What if $b > 10$? What are the digits?

HEX notation is base 16

$\underline{\text{Digits}}$: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \underset{10}{A}, \underset{11}{B}, \underset{12}{C}, \underset{13}{D}, \underset{14}{E}, \underset{15}{F}\}$

$(6D)_{16} = 6 \cdot 16^1 + \underline{13}\, 16^0 = 6 \cdot 16 + 13 = 109$

$(1EF)_{16} = 1 \cdot 16^2 + 14 \cdot 16^1 + 15 \cdot 16^0$

$= 16^2 + 14 \cdot 16 + 15$

Easy to convert between binary (base 2) and HEX (base 16)
(because 16 is a power of 2: $2^4 = 16$).

$(10110110)_2 = (B6)_{16}$

$AB = \underbrace{1010}_{A}\ \underbrace{1011}_{B}$

Easier for humans to read + remember a byte of data expressed in HEX (as opposed to binary).

Converting decimal to base b:

$$\underbrace{1862} = \underbrace{5 \cdot 7^3 + 2 \cdot 7^2 + 1 \cdot 7^1}_{\text{multiple of}} + \underbrace{6 \cdot 7^0}_{\substack{6 \\ \{0, \ldots, 6\}}}$$

Base 7 expansion of 1862 :

$$[\text{Base 7 exp of } \underline{1862 \text{ div } 7}]\ [1862 \text{ mod } 7]$$

$$(5 \cdot 7^2 + 1 \cdot 7^1 + 1)$$

Binary expansion of 56

$$[\text{bin exp of } 56 \text{ div } 2]\ [56 \text{ mod } 2]$$

| | | | | | |
|---|---|---|---|---|---|
| | | | [28] | | 0 |
| | | [14] | | 0 | 0 |
| | [7] | 0 | | 0 | 0 |
| [3] | 1 | 0 | | 0 | 0 |

$$(1\ 1\ 1\ 0\ 0\ 0)_2 = 56$$

Base 5 expansion of 73

| | | |
|---|---|---|
| | [14] | 3 |
| [2] | 4 | 3 |

$$(2\ 4\ 3)_5 = 73$$

Expansion $(n, b)$ // $n, b$ integers. $b > 1$, $n > 0$.
// outputs base b expansion of n in reverse order.

```
    Output (n mod b)
    If (n div b > 0)
        Expansion (n div b, b)
End.
```

How many digits required to express n base b?

What is the largest # uses k digits base b?

$$(\underbrace{[b-1][b-1] \cdots [b-1]}_{k})_b$$

$k = 5 \quad b = 8.$

$$\begin{array}{r} 77777 \\ +1 \\ \hline (100000)_8 \end{array}$$

$\underbrace{10 \cdots 0}_{k}$

$n \leq b^k - 1$

$n + 1 \leq b^k$

$\log_b(n+1) \leq \log_b(b^k) = k$

$\Rightarrow \log_b(n+1) \leq k$

$k = \lceil \log_b(n+1) \rceil$ → # digits base b to express n.

## Fast modular exponentiation

Power $(a, e, n)$ // $a, e$ integers in $\mathbb{Z}_n$

// Compute $a^e \bmod n$

If $(e = 0)$ return 1.

If ($e$ is even)

Return ( Power $(a, e/2, n)^2 \bmod n$ )

If ($e$ is odd)

Return ( Power $(a, \lfloor e/2 \rfloor, n)^2 \cdot a \bmod n$ )

End.

Compute: $(78)^{57} \bmod 5$

Power $(78, 57)$

Power $(78, 3)$

$57 \to 28 \to 14 \to 7 \to 3 \to 1$

$78^1 \bmod 5 = 3$

$(3^2 \cdot 78) \bmod 5$

$4 \cdot 3 = 2$

$78^7 \bmod 5 = 2^2 \cdot 78 \bmod 5$

$= 4 \cdot 3 \bmod 5 = 2.$

$2^2 \bmod 5 = 4$

$4^2 \bmod 5 = 1.$

$1^2 \cdot 78 \bmod 5 = 3$