Math 321

4.2 Integer Representation (base b numbers)

$$n = a_k b^k + \cdots + a_2 b^2 + a_1 b + a_0 \qquad 0 \le a_i < b$$

$$n = (a_k, \ldots, a_2, a_1, a_0)_b$$

ex $(1,2,3)_{10} = 1 \cdot 10^2 + 2 \cdot 10 + 3$

$(1,2,3)_5 = 1 \cdot 5^2 + 2 \cdot 5 + 3$

base 8 $(1,0,2,7,3)_8 = 1 \cdot 8^4 + 0 \cdot 8^3 + 2 \cdot 8^2 + 7 \cdot 8 + 3$

$8^4 \quad 8^3 \quad 8^2 \quad 8 \quad 1$

$(1,0,2,0,3)_{10} = 10,203$

---

add $(2x+3) + (x+7) = 3x + 4$

$$\begin{array}{r} {\scriptstyle 1} \\ (1,2,3)_8 \\ +\,(7,0,6)_8 \\ \hline (1,0,3,1)_8 \end{array} \qquad \begin{array}{r} (3)_8 \\ +\,(6)_8 \\ \hline (1,1)_8 \end{array}$$

---

mult: $(2+3a)(4-a) = 2 \cdot 4 + 2 \cdot (-a) + 3a \cdot 4 + 3a(-a)$

$((1 \cdot 10 + 3) \cdot (2 \cdot 10 + 1))$

$13 \cdot 21$

$$\begin{array}{r} 1\,3 \\ \times\ 2\,1 \\ \hline 1\,3 \\ 2\,6\,0 \\ \hline 2\,7\,3 \end{array}$$

(1)

$(1,3)_4$

(ex) $\times\ (2,1)_4$

$(1,3)_4$

$(3,2,0)_4$

$(3,3,3)_4$

Change base

$n = (a_k, \dots, a_2, a_1, a_0)_b$

1st (to 10) $n = a_k b^k + \dots + a_2 b^2 + a_1 b + a_0$

(ex) $(3,3,3)_4 = 3\cdot 4^2 + 3\cdot 4 + 3 =$

4^2 4 1

2nd to base b — given $n = (a_k, \dots, a_2, a_1, a_0)_b$ — find these

$n = a_k b^k + \dots + a_2 b^2 + a_1 b + a_0$

$n = b(a_k b^{k-1} + \dots + a_2 b + a_1) + a_0$

$n = b \cdot q + r$

q: n div b — r: n mod b

(ex) $n = 55$ in base 4 $\quad (3,1,3)_4$

$55 = 4\cdot(13) + 3$

$13 = 4\cdot(3) + 1$

$3 = 4\cdot(0) + 3$

4^2 4 1

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

$= 3\cdot 16 + 7 = 55$

So $(5,5)_{10} = (3,1,3)_4$

Need later: $(b^n) \bmod m = c \qquad b \leftrightarrow c$

Use: $(x \cdot y) \bmod m = ((x \bmod m)(y \bmod m)) \bmod m$

(ex) $2^{100} \bmod 5 = (2 \cdot 2 \cdot 2 \cdot 2 \cdots 2) \bmod 5$

loop 1 to 100 $\quad 2 \bmod 5 = 2$

$2 \times 2 \bmod 5 = 4$

$(4 \times 2) \bmod 5 = 3$

$100 = (1,1,0,0,1,0,0)_2$

$2^6 \; 2^5 \; 2^4 \; 2^3 \; 2^2 \; 2 \; 1$

$100 = 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 0$

$100 = 2(50) + 0$

$50 = 2(25) + 0$

$25 = 2(12) + 1$

$12 = 2(6) + 0$

$6 = 2(3) + 0$

$3 = 2(1) + 1$

$1 = 2(0) + 1$

$2^{100} = 2^{1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 0}$

$= (2^{1 \cdot 2^6})(2^{1 \cdot 2^5})(2^{0 \cdot 2^4})(2^{0 \cdot 2^3})(2^{1 \cdot 2^2})(2^{0 \cdot 2})(2^0)$

$= (2^{2^6})^1 (2^{2^5})^1 (2^{2^4})^0 (2^{2^3})^0 (2^{2^2})^1 (2^2)^0 (2)^0$

$= (\;)^1 (\;)^1 (\;)^0 (\;)^0 (\;)^1 (\;)^0 (\;)^0 \bmod 5$

$= (1)^1 (1)^1 (1)^0 (1)^0 (1)^1 (4)^0 (2)^0 \bmod 5 = \boxed{1}$

(square)

$(102)^{101} \bmod 9$

$101 = (1,1,0,0,1,0,1)_2$

$(4)^1 (2)^1 (4)^0 (2)^0 (4)^1 (2)^0 (\cancel{102})^1 \bmod 7$

$7 \overline{)102}$ → 14, 7, 32, 28, 4 → $102 \underset{7}{\equiv} 4$

$4 \cdot 4 \cdot 4$ → $\times 4$: $16 \underset{7}{\equiv} 2$

$= \boxed{2}$

$(4)^1 (2)^1 \cancel{(4)^0} \cancel{(2)^0} (4)^1 \cancel{(2)^0} (4)^1 \bmod 7 = \boxed{2}$

$16 \underset{7}{\equiv} 2$ → 4; $16 \underset{7}{\equiv} 2$

Example 12 p. 254

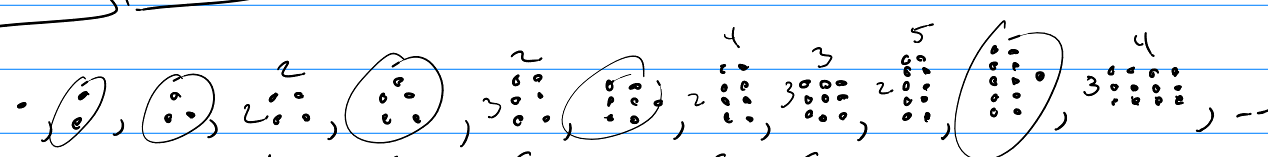
$3^{644} \bmod 645$

$644 = (1010000100)_2$

$(111)^1 (81)^0 (396)^1 (126)^0 (486)^0 (66)^0 (111)^0 (81)^1 (9)^0 (3)^0 \bmod 645$

$81^2 = 6561 \underset{645}{\equiv} 111$

Primes 9.3



1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, ...

1 is special!

Prime: only factors are $1 \cdot p$

Composite: not prime

$c = a \cdot b \quad 2 \le a \le c-1$

$\quad\quad\quad\quad\; 2 \le b \le c-1$

Fund. thm of Arithmetic

for all numbers $n \geq 2$ n is prime or can be written as a unig. prod. of primes written in non dec. order.

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, ...
(2), (3), (2^2), (5), (2·3), (7), (2^3), (3^2), (2·5), (11), (2^2·3), (13), (2·7), ...

Prime Sieve's

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~~

thm if n is composite it has a prime factor $\leq \sqrt{n}$