24 JANUARY 2012

Recall:

=> $\varphi(n)$ = # of units in $\mathbb{Z}/n\mathbb{Z}$

units $\not\in$: $x \in$ unit if and only if $xy \equiv 1 \pmod p$

= # of items on $\{0, 1, \ldots, n-1\}$ that are coprimes of n.

=> $\varphi(ab) = \varphi(a) * \varphi(b)$ if $\gcd(a,b) = 1$

Proof

units in $\mathbb{Z}/ab\mathbb{Z}$ are composed of units in $\mathbb{Z}/a\mathbb{Z}$ and $\mathbb{Z}/b\mathbb{Z}$

Take c, $\gcd(a \cdot b, c) = 1$

=> $\gcd(a \cdot c) = 1 \quad \wedge \quad \gcd(b \cdot c) = 1$

then $\underbrace{c \bmod (ab)}_{\text{units in } \mathbb{Z}/ab\mathbb{Z}} \longrightarrow (c \bmod a, c \bmod b)$ units in $\mathbb{Z}/a\mathbb{Z}$, units in $\mathbb{Z}/b\mathbb{Z}$

Theorem: Chinese Remainder Theorem

Given a, b with $\gcd(a,b) = 1$

Pick cosets $r \bmod a$

$s \bmod b$

Then there is exactly one coset $t \bmod ab$ such that

$t \bmod a = r \bmod a$ and $t \bmod b = s \bmod b$

This says:

system eq: $x - r$ is divisible by a

$x - s$ is divisible by b

has a solution $t, t+ab, t+2ab, \ldots$.

In fact, we find t:

→ find an inverse for $a \bmod b$ (call m) and $b \bmod a$ (call n).

→ then, $t = rbn + sam$

ex.

$a = 2$, $b = 3$

solve: $x = 1 \bmod 2$ $\quad r = 1$

$x = 2 \bmod 3$ $\quad s = 2$

=> Find inverse for $a \bmod b$, $b \bmod a$: $2 \bmod 3$ $\quad 3 \bmod 2$.

inv $2 \bmod 3 = 2 \bmod 3 \quad m = 2$

inv $3 \bmod 2 = 3 \bmod 2 \quad n = 1$

$t = rbn + sam = 1 \cdot 3 \cdot 1 + 2 \cdot 2 \cdot 3$

$\times \boxed{= 11}$.

How does the formula work?

Reduce $t = rbn + sam$

$t \bmod a = (rbn + sam) \pmod a = rbn \bmod a = r \cdot 1 \bmod a$

(b is the inverse of n)

$t \bmod b = sam \bmod b = s \cdot 1 \bmod b$

Divisibility Test

Fact: In order for n to be multiple of three, the sum of the digits should be divisible by 3

Pf $n = a_k a_{k-1} \ldots a_0$ (in decimal form, each a_i representing a digit)

$= a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \ldots 10^k a_k$

we reduce by $n \bmod 3$, which would yield:

$n \bmod 3 = a_k \cdot 1^k + \ldots + a_1 \cdot 1 + a_0 \pmod 3 = \Sigma a_i \bmod 3$.

Therefore for $3 \mid n$, $\Sigma a_i \bmod 3 \equiv 0$.

2. Same rule for 9:

$9 \mid n \iff 9 \mid$ sum of digits

3. ~~Divisibility of n mod 11~~: 11:

$n \bmod 11 = a_k \cdot 10^k + \ldots + a_1 10^1 + a_0 \pmod{11}$

$= (a_k \cdot -1) +/- \ldots + a_2 - a_1 \cdot 1$

↳ this result comes from fact that $10 \bmod 11 = 9$ or -1

$100 \bmod 11 = 1$ ...

$11 \mid n \iff 11 \mid$ alternating sum of digits

Theorem: Let p be prime.

Then $a^p = a \pmod p$ for any $a \in \mathbb{Z}$ (Fermat's Little Theorem)

Pf: 2 cases:

(1) $p \mid a$: (supposedly this is easy to prove... but I couldn't catch what he meant)

If $p \nmid a$, then $\gcd(p,a) = 1$

Then, a is a unit of mod p.

Looking at the list of units of mod p : $\{1, 2, \dots, p-1\}$.

and compare to $\{a, 2a, \dots, a(p-1)\}$

Since no number divides p, $\{1, 2, \dots, p-1\} = \{a, 2a, \dots, (p-1)a\} \bmod p$.

$$\Rightarrow 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) = a \cdot 2a \cdot \dots a(p-1) \bmod p$$

$$1 \cdot 2 \cdot 3 \dots (p-1) = a^{p-1}(1 \cdot 2 \cdot \dots (p-1)) \bmod p$$

$$1 = a^{p-1} \bmod p.$$

$$a = a^p \bmod p. \quad \checkmark$$

PROBABILITY.

INTRODUCTION: Deck of Cards

→ Significant Hands

: XXXX Y : 4 of a kind

XXX YZ : 3

XXX YY : Full House

XX YY Z : 2 pairs

XX Y Z W : pair ... etc.

General Principle

→ make an algorithm that produces a desired hand

→ count # runs and "overcounts"

→ Determine # of outputs

Ex

- # of outputs for ~~all~~ any hands:

$52 \cdot 51 \cdot 50 \cdot 48 \cdot 49$ = # of getting 5 cards

note: there are many redundancies and "overcount" in above count.

5! ways of getting ~~5 cards~~ a particular set of 5 cards.

Thus: $\frac{52 \cdot 51 \cdot 50 \cdot 49 \cdot 48}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = \frac{\#\text{ of runs}}{\#\text{ of rus per hand}} = \#\text{ of hands}$

ex 4 of a kind

1. pick X = 13 (13 possible 4 of a kind types: {A, 2, 3, ..., K})
2. choose any Y = 48

= there exists 13×48 ~~4 of a kind~~ ways to get a 4-kind

ex Full House

1. Choose X → 13
2. Choose Y → 12
3. Choose 3 of 4 Xs → 4 (4 ways to choose 3 out of 4 cards)
4. Choose 2 of 4 Ys → 6 (6 " 2 ")

$= 13 \cdot 12 \cdot 4 \cdot 6$ ways to get a Full House

NOTE: There is no redundancies in above calc. we were thinking of a specific full house... and we accounted for redundancies in our # of possibilities.

Q: If you have to choose k things from a given list of n things, how many ways are there?

$$\Rightarrow \frac{n(n-1)(n-2)\cdots(n-k+1)}{(k-1)} = \binom{n}{k}$$

Choosing 2 pairs #ways

1. pick X = 13
2. choose Y = 12
3. Choose Z and pick 1 = 44 (11·4)
4. Choose 2 out of 4 Xs = 6
5. Choose 2 out of 4 Ys = 6

⇒ is there overcount in this algorithm? Yes! there is ambiguity of X, Y: If X=A and Y=2, then choosing Y=A X=2 would yield same hand. Thus overcount by factor of 2.

⇒ Alternatively, 1, and 2 can combine:
- choose X and Y at once: $\binom{13}{2} = \frac{13 \cdot 12}{(2)}$ — overcount factor.