





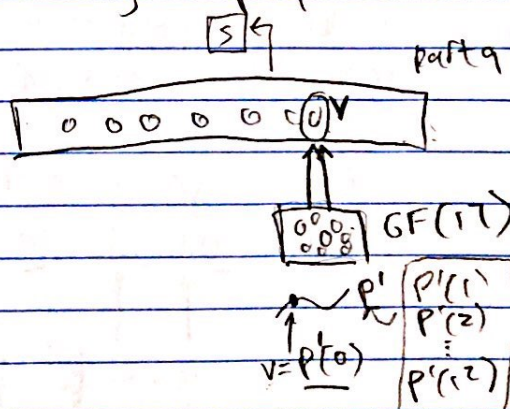
- 2 Given  $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  for  $a_0, \dots, a_n \in \mathbb{Z}$ , if  $a_0, a_n \neq 0$  prove every rational solution  $\frac{p}{q}$  has  $pl | a_0$  and  $q | a_n$  for  $\gcd(p, q) = 1$

- 3 (a) All 193 countries agree, or SG + 55 countries agree (b) Extra level of security: each country has 12 representatives that must agree

n ppl polynomial deg. (n-1)

a polynomial having degree 192, distribute its values at  $x=1, x=2, \dots, x=193$ . Encode the secret as the value of the polynomial at  $x=0$ .

every country has its own polynomial  $P$  where its secret is encoded as  $P(0)$ , and we distribute 12 values of this polynomial  $P$  to each member of that country's delegation. Also  $P$  is a degree-11 polynomial here



$$\begin{array}{r} 193 \\ - 55 \\ \hline 138 \end{array}$$

give SG 138 points, st if he meets w/ 55 countries it has enough info to recover the secret.

$P = 367$  ← values @ points 1 thru 138 to SG  
← values @ points 139 thru 332 distribute those to other countries