CS70 Disc 3C: tinyurl.com/frank-discussion 7/8/2020

1 (a) (i) min/max num. roots for f+g

min: 0 $f=x^2+1$ $g=x^2+1$

f+g has no solutions

max: $\max(\deg(f),\deg(g))$

$f=-g$ 0 (infinite solutions)

(ii) min/max num. roots for f·g

min: 0 $f=g=(x^2+1)$

$(x^2+1)(x^2+1)$

max: $\deg(f)+\deg(g)$

$f=x^4$ $g=x^3$

$f\cdot g=x^7$

(iii) min/max num. roots for f/g, assuming it's a polynomial

min: 0

$f(x)=g(x)(x^2+1)$

$f(x)/g(x)=x^2+1$,

max: $\deg(f)-\deg(g)$

$f=x^4$ $g=x^3$ $\frac{f}{g}=x^1$

2 min glow
5 min break
20 min go over

(b) (i) If $\forall x$ $f\cdot g=0$, is it true that either $f=0$ or $g=0$?

Key Insight: in general, $\forall x$ such that $f\cdot g(x)=0$, either $f(x)=0$ or $g(x)=0$

$f=x^{p-1}-1$ $g=x$

$f\cdot g=x(x^{p-1}-1)$

FLT: $x^{p-1}\equiv 1 \pmod p$, $x\not\equiv 0 \pmod p$

$\forall x$ $0\le x\le p-1$ $f\cdot g(x)=0$

Case 1: $x=0 \Rightarrow f\cdot g(x)=0$

Case 2: $x\neq 0 \Rightarrow$ FLT says $x^{p-1}-1=0$

(ii) How many f of degree exactly $d<p$ are there such that $f(0)=a$ for some fixed $a\in\{0,1,\dots p-1\}$?

Common Misconception:
A polynomial of degree d is specified by its values at (d+1) points.

Here we are given that (0, a) is a point, so to determine the rest of the polynomial, we need to pick its values at d other points. p^d

(c) How many polynomials in GF(5) such that $f(0)=1$, $f(2)=2$, and $f(4)=0$?

GF(5) has possible x-values incl. equal to 0, 1, 2, 3, or 4 (0–4)

$5\times 5=25$

$P(x)=a_d x^d+a_{d-1}x^{d-1}+\dots+a_1x^1+a_0$ (fixed constant)

$a_d\neq 0$

d-1 coefficients (0–(p-1) inclusive)

$(p-1)p^{d-1}$ ← p values inside this range

5:38

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 $p | a_0$ 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

2 min alone
5 mm break
15 min group

n ppl polynomial deg. (n-1)

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

193
− 55
138

1 1
139
+193
332

give SG 138 points, s.t. 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

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