sundry:

Fatima Atty Ibrahim fibrahimb@berkeley.edu
Anais Miller anais.miller@berkeley.edu
Nada Al-Alusi nada118@berkeley.edu

I certify that all solutions are entirely in my words and that I have not looked at another students' solutions. I have credited all external sources in this write up

2. a) (0,1)

(1,1)

(2,3)

$$\Delta_1 x = \frac{(x-1)(x-2)}{(0-1)(0-2)} = \frac{x^2-3x+2}{2}(1) = \frac{x^2}{2} - \frac{3}{2}x + 1$$

$$\Delta_2 x = \frac{(x-0)(x-2)}{(1-0)(1-2)} = \frac{x^2-2x}{-1}(1) = -x^2 + 2x$$

$$\Delta_3 x = \frac{(x-0)(x-1)}{(2-0)(2-1)} = \left(\frac{x^2-x}{2}\right)(3) = \frac{3}{2}x^2 - \frac{3}{2}x$$

$$= x^2 - x + 1$$

b) (0,1)

(1,1)

(2,3)

(-1,3)

from part a $f(x) = x^2 - x + 1$, have to check if $(-1,3)$ passes

plug in → $3 = (-1)^2 - (-1) + 1 = 1+1+1$ ✓

$\boxed{\text{True}}$

c) $f(x) = x^2 - x + 1$ (same reasoning as part b)

$0 = (-1)^2 - (-1) + 1 \neq 1+1+1$ ✗ $\boxed{\text{False}}$

d) (x_1, y_1) (x_2, y_2) (x_3, y_3) (x_4, y_4)

want to see if exists polynomial $P(x)$ w/ degree 2

First use Lagrange interpolation to create degree 2 polynomial from 3 of the 4 points and then plug the last point into the equation → point is found on that polynomial if the equation is true, return yes else no

```
def degree_2-poly ( the four points ):
poly= solve lagrange (point 1, point 2, point 3)
if poly( point 4 _x) == point4_y
    return 'yes'
else
    return 'no'
```

3. For every prime p, polynomial over GF(p), even polynomial degree $\geq p$ = polynomial of degree at most $p-1$

a)

Fermat's Little Theorem: For any prime p and any $a \in \{1, 2 \ldots p-1\}$ we have $a^{p-1} \equiv 1 \bmod p$

(a) $a^{p-1} \equiv 1 \bmod p$ (a) multiply both sides by 'a'

$\forall a$ $a^p \equiv a \bmod p$ we get

which means for any a^x such that $x \geq p$

this is equivalent to a^y $y \in \{0, 1, \ldots p-1\}$

with max degree $(p-1)$

b) Every polynomial is over GF(p) $\rightarrow$ polynomial mod p

ex: polynomial $p(x)$ with max degree $p-1$ is defined by p points

polynomial $d(x)$ with max degree d where $d > p-1$

and defined by $d+1$ points

If $d+1$ points for $d(x)$ = p points and $d+1-p$ points

then $d+1-p$ points are not unique

equal # less than p because $d+1-p \bmod p$ is smaller than p

So every polynomial over GF(p) is equal to polynomial of degree of max p

Scanned by CamScanner

4. a) gcd $(A(x), B(x)) = D(x)$ if $A(x), B(x)$ can be divided by $D(x)$

gcd - highest degree poly. that divides both $A(x)$. $B(x)$

compute gcd $(A(x), B(x))$

quotient remainder

need to find soln to: $A(x) = B(x)\,Q_0(x) + R_0(x)$ [long division]

assume degree $A(x)$ > degree $B(x)$

because there also exists $C(x)$ that divides $A(x)$, $B(x)$, $R_0(x)$.

gcd $(A(x), B(x))$ is equal to gcd $(B(x), R_0(x))$

we can recurse on this, setting A to the next B value and B to the next remainder until our B value reaches zero, which at that point you stop, and the gcd will have been found.

b) $P(x) = x^4 - 1$ Prove no polynomials $A(x)$ $B(x)$ such that

$Q(x) = x^3 + x^2$ $A(x)P(x) + B(x)Q(x) = 1$

$P(x) = (x^2+1)(x-1)(x+1)$] $\underline{\text{gcd } (P(x), Q(x)) = x+1}$

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

extended GCD for polynomial

$\gcd(x^4-1, x^3+x^2) = (x^3+x^2)(x-1) + (x^2-1)$

$$\begin{array}{r|l} & x-1 \\ \hline x^3+x^2 & x^4 \quad -1 \\ & -x^4 + x^3 \\ \hline & -x^3 - 1 \\ & x^3 + x^2 \\ \hline & x^2 - 1 \end{array}$$

$x-1$, R x^2-1

$\gcd(x^3+x^2, x^2-1) = (x^2-1)(x+1) + (x+1)$

$$\begin{array}{r|l} x^2-1 & x^3 + x^2 \\ & -x^3 - x \\ \hline & -x^2 + x \\ & x^2 + 1 \\ \hline & x + 1 \end{array}$$

$\gcd(x^2-1, x+1) = (x+1)(x-1) + 0$

$$\begin{array}{r|l} & x-1 \\ \hline x+1 & x^2 - 1 \\ & -x^2 + x \\ \hline & -x - 1 \\ & x + 1 \\ \hline & 0 \end{array}$$

$\gcd((x+1), 0) = (x+1)$

$$A(x)P(x) + B(x)Q(x) = \underbrace{(x+1)(A(x)P_n(x) + B(x)Q_n(x))}_{\text{has to be polynomial degree } \geq 1} = 1$$

but $(x+1)(A(x)P_n(x) + B(x)Q_n(x)) \neq 1$

so there is a contradiction $\rightarrow$ $A(x)P(x) + B(x)Q(x) \neq 1$ for all x

c) $A(x)P(x) + B(x)Q(x) = x+1$

- work backwards with extended gcd output of part b

$$x+1 = (x^3+x^2) - (x+1)(x^2-1)$$
$$= (x^3+x^2) - (x+1)\left[(x^4-1) - (x^3+x^2)(x-1)\right]$$
$$= (x^3+x^2) - (x+1)(x^4-1) + (x+1)(x^3+x^2)(x-1)$$
$$= -(x+1)(x^4-1) + x^2(x^3+x^2)$$

$A(x) = -(x+1)$ $\qquad$ $B(x) = x^2$

Scanned by CamScanner

5a. Properties of GF(p)

proof by contrapositive

want to prove: if $p(x), q(x)$ are polynomials (real) and $\forall x$ $p(x) \cdot q(x) = 0$

then either $p(x) = 0$ <u>OR</u> $q(x) = 0$

contrapositive: $\forall x$ $p(x) \neq 0$ and $\forall x\, q(x) \neq 0$

then $\exists x$ $p(x) \cdot q(x) \neq 0$

so $p(x) \neq 0$ $q(x) \neq 0$ (A nonzero polynomial degree d has at most d roots)

$\rightarrow$ degree $(p(x))$ = # x's such that $p(x) = 0$

$\rightarrow$ degree $(q(x))$ = # x's such that $q(x) = 0$

$p(x)$ and $g(x)$ have infinitely many values of x that are nonzeroes

so exists $p(x') \neq 0$ and $q(x') \neq 0$ for a same x' value

$p(x') \neq 0$ non zero $p(x')\, q(x') \neq 0$

$q(x') \neq 0$ nonzero (nonzero)(nonzero) $\neq 0$ ✓

Thus we proved by contrapositive, the statement

$\forall x$ $p(x) \cdot q(x) = 0$, $p(x) = 0 \vee q(x) = 0$

5b. <u>Finite fields GF(p)</u> part a is false

if $p(x), q(x)$ polynomials $\forall x$ $p(x) \cdot q(x) = 0$

either $p(x) = 0$ or $q(x) = 0$

Counter example: Fermat's Little Theorem - any $x \in \{1, 2, \ldots, p-1\}$

$$x^{p-1} = 1 \pmod p$$

$$x\,(x^{p-1}) \equiv 1\,(x) \pmod p$$

$$x^p \equiv x \bmod p$$

$$x^p - x = 0, \quad x^p = x$$

if we factor out $x \rightarrow x$, $x^{p-1} - 1$

$$x \neq 0 \qquad x^{p-1} - 1 \neq 0$$

$$(x)(x^{p-1} - 1) = 0$$

So for finite fields, Claim in part a is false

6\. a) $\Delta_i(x)$ polynomials for $i \in \{1,2,3\}$

$$\Delta_1(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{1}{2}x^2 - \frac{5}{2}x + 3 \pmod 5 \equiv 3x^2 - 0 + 3$$

$$\Delta_2(x) = \frac{(x-1)(x-3)}{(2-1)(2-3)} = -x^2 + 4x - 3 \pmod 5 \equiv 4x^2 + 4x + 2$$

$$\Delta_3(x) = \frac{(x-1)(x-2)}{(3-1)(3-2)} = \frac{1}{2}x^2 - \frac{3}{2}x + 1 \pmod 5 \equiv 3x^2 + x + 1$$

b) $P(x) = 2\Delta_1 + 4\Delta_2 + 3\Delta_3$

$2(3x^2 - 0 + 3) + 4(4x^2 + 4x + 2) + 3(3x^2 + x + 1)$

$6x^2 + 6 + 16x^2 + 16x + 8 + 9x^2 + 3x + 3$

$31x^2 + 19x + 17 \mod 5$

$x^2 + 4x + 2$

c) $c_0 + c_1 x + c_2 x^2$ $(1,2)$ $(2,4)$ $(3,3)$

x y

$P(1) = 2 = c_0 + c_1 + c_2 \mod 5$

$P(2) = 4 = c_0 + 2c_1 + 4c_2 \mod 5$

$P(3) = 3 = c_0 + 3c_1 + 9c_2 \mod 5$

d) $4 = c_0 + 2c_1 + 4c_2$

$3 = c_0 + 3c_1 + 4c_2$

$1 = -1c_1 \mod 5$

$c_1 = -1 \mod 5 \to 4$ $P(x) = 2 + 4x + x^2$

$c_2 = 1$

$c_0 = 2$

$2 = c_0 - 1 + c_2$

$-4 = -c_0 + 2 - 4c_2$

$-2 = 1 - 3c_2$

$-3 = -3c_2$

$1 = c_2$

$2 = c_0 + -1 + 1$

e) $x^2 + 4x + 2$