Kevin Chau

Homework 6

Problem 1 a) $n=1$: $0 \Rightarrow 0$ $\quad 1 \Rightarrow 2^0 = 1$ [2 messages]

$n=2$: $00 \Rightarrow 0$ $\quad 10 \Rightarrow 2^1 = 2$ [4 messages]

$01 \Rightarrow 2^0 = 1$ $\quad 11 \Rightarrow 2^1 + 2^0 = 3$

$n=3$: $000 \Rightarrow 0$ $\quad 011 \Rightarrow 2^1 + 2^0 = 3$

$001 \Rightarrow 2^0 = 1$ $\quad 110 \Rightarrow 2^2 + 2^1 = 6$ [8 messages]

$010 \Rightarrow 2^1 = 2$ $\quad 101 \Rightarrow 2^2 + 2^0 = 5$

$100 \Rightarrow 2^2 = 4$ $\quad 111 \Rightarrow 2^2 + 2^1 + 2^0 = 7$

This encoding is just how we get from binary numbers to decimal numbers. With n bits, how many binary numbers are there? $\boxed{2^n \text{ messages}}$

Our messages are in the range $[0, 2^n - 1]$.

b) 5 different messages (for $n \geq 3$). We always know that $c=0$ will always be an encoding, so $2^0 = 1$ is always a valid message. Now for any $n \geq 3$, we will always have $c = 1, 2, 3, 4$ at least. Any power of 2 is always an even number. $2^1 \equiv 2 \bmod 10$, $2^2 \equiv 4 \bmod 10$, $2^3 \equiv 8 \bmod 10$, $2^4 \equiv 6 \bmod 10$

Since 2, 4, 6, 8 are all of the even digits, and any encoding with $n \geq 3$ has $c = 1, 2, 3, 4, 0$, there are only 5 messages.

c) a must be coprime with 2^n.

Proof: if "a" is coprime with 2^n, then its gcd with 2^n is just 1. Hence "a" has a multiplicative inverse mod 2^n. From lecture 5, we know that a mod m number with a multiplicative inverse multiplied by all the numbers less than m results in a set that is just a permutation of all numbers less than m. So if we want all numbers $c \in [0, 2^n - 1]$ to be uniquely encoded after multiplying by "a," then "a" has to be coprime with 2^n.

d) With two primes p, q, choose a third prime r. Now $N = pqr$ and the encryption key e is coprime with $(p-1)(q-1)(r-1)$. Again, the decryption key $d \equiv e^{-1} \bmod (p-1)(q-1)(r-1)$.

We need to prove that $E(x) = x^e \bmod N$ and $D(y) = y^d \bmod N$

are such that $D(E(x)) \equiv x \bmod N$.

Proof: show that $(x^e)^d \bmod N \equiv x \bmod N$

By defintion of d, $ed \equiv 1 \bmod (p-1)(q-1)(r-1)$

so $ed = 1 + k(p-1)(q-1)(r-1)$

$\Rightarrow \underline{x^{ed} - x = x^{1+k(p-1)(q-1)(r-1)} - x = x(x^{k(p-1)(q-1)(r-1)} - 1)}$

If this equation is equivalent to $0 \bmod N$, we have proven our claim. (it is divisible by N).

Case 1 If x is a multiple of p, then the expression is congruent mod p

case 2 If x is ~~not~~ not a multiple of p, then by FLT we know

$x^{p-1} \equiv 1 \bmod p$ so $(x^{p-1})^{k(q-1)(r-1)} - 1 \equiv 1^{k(q-1)(r-1)} - 1 \equiv 1 - 1 \equiv 0 \bmod p$.

- By symmetric arguments, primes q and r also divide the expression. Since p, q, r divide it and they are prime, it is also divisible by their product N. Thus $x^{ed} \equiv x \bmod N$.

e) $E(x) = x^{e/2} \bmod N = x^{e(2^{-1}) \bmod N} \bmod N = y$

Since all we need to do is have $D(y) = y^{d'} \equiv x \bmod N$, we see that d' has to be $2d$ to cancel out the $2^{-1} \bmod N$. So $y^{d'} = x^{ed} \equiv x \bmod N$

Proof:

$$D(E(x)) = (x^{e(2^{-1}) \bmod N})^{d'} \bmod N \equiv x \bmod N$$

$$= x^{e(2^{-1})d' \bmod N} \bmod N \equiv x \bmod N$$

$$\Rightarrow d'(2^{-1}) \bmod N \equiv d \bmod N$$

$$\cancel{2} d' \cancel{(2^{-1})} \bmod N \equiv 2d \bmod N$$

$$\boxed{d' \equiv 2d \bmod N}$$

Problem 2

$16x + 5y = 14 \mod 21$
$9x + 11y = 4 \mod 21$

a) $16x+5y = 14 \pmod 3 \Rightarrow \boxed{1x + 2y = 2 \pmod 3}$
$9x+11y = 4 \pmod 3 \Rightarrow \boxed{0x + 2y = 1 \pmod 3}$
$\Rightarrow y \equiv 2 \cdot 1 \mod 3 \equiv 2 \mod 3$
$x \equiv 2 - 2(2) \mod 3 \equiv 1 \mod 3$

$16x+5y = 14 \mod 7$
$9x+11y = 4 \mod 7$
$\Rightarrow \boxed{\begin{array}{ll} 2x+5y = 0 & (\mathrm{mod}\ 7) \\ 2x+4y = 4 & (\mathrm{mod}\ 7) \end{array}}$

b) (mod 3): $\boxed{\begin{array}{l} x \equiv 1 \mod 3 \\ y \equiv 2 \mod 3 \end{array}}$

(mod 7): $2x + 4y = 4 \mod 7 \Rightarrow 2x = 4 - 4y \mod 7$
$x \equiv 2^{-1}(4-4y) \mod 7$
$x \equiv 4(4-4y) \mod 7$
$x \equiv 16 - 16y \mod 7 \equiv 2 - 2y \mod 7$
$\Rightarrow 2(2-2y) + 5y \equiv 0 \mod 7$
$\Rightarrow 4 - 4y + 5y \equiv 0 \mod 7 \Rightarrow \boxed{y \equiv -4 \mod 7 \equiv 3 \mod 7}$
$\Rightarrow \boxed{x \equiv -4 \mod 7 \equiv 3 \mod 7}$

c) $x \equiv 1 \mod 3 \Rightarrow \{1, 4, 7, 10, 13, 16, 19, 22 \ldots\}$
$x \equiv 3 \mod 7 \Rightarrow \{3, 10, 17, 21, \ldots\}$
$\boxed{x \equiv 10 \mod 21}$

$y \equiv 2 \mod 3 \Rightarrow \{2, 5, 8, 11, 14, 17, 20, 23, \ldots\}$
$y \equiv 3 \mod 7 \Rightarrow \{3, 10, 17, 21, \ldots\}$
$\boxed{y \equiv 17 \mod 21}$

Check: $16(10) + 5(17) = 160 + 85 \equiv 14 \mod 21$ ✓
$9(10) + 11(17) = 90 + 187 = 277 \equiv 4 \mod 21$ ✓

Note: Chinese remainder theorem says our answers to part b can always be combined to make a solution in mod 21

Problem 3 Polynomial Interpolation

a) $\{(0,1),(1,-2),(3,4),(4,0)\}$

$P(x)$ is degree 3 $\Rightarrow a_3x^3+a_2x^2+a_1x+a_0 = P(x)$

$(0,1)$: $a_0 = 1$

$(1,-2)$: $a_3+a_2+a_1+a_0 = -2$
$(3,4)$: $27a_3+9a_2+3a_1+a_0 = 4$
$(4,0)$: $64a_3+16a_2+4a_1+a_0 = 0$

3 equations, 3 unknowns a_3, a_2, a_1

$$\Rightarrow \left[\begin{array}{ccc|c} 1 & 1 & 1 & -3 \\ 27 & 9 & 3 & 3 \\ 64 & 16 & 4 & -1 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 1 & 1 & -3 \\ 0 & -18 & -24 & 84 \\ 0 & -48 & -60 & 191 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 1 & 1 & -3 \\ 0 & 3 & 4 & -14 \\ 0 & 48 & 60 & -191 \end{array}\right]$$

$$\sim \left[\begin{array}{ccc|c} 1 & 1 & 1 & -3 \\ 0 & 3 & 4 & -14 \\ 0 & 0 & -4 & 33 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 0 & 0 & -13/12 \\ 0 & 1 & 0 & 19/3 \\ 0 & 0 & 1 & -\frac{33}{4} \end{array}\right]$$

So $\boxed{P(x) = -\tfrac{13}{12}x^3 + \tfrac{19}{3}x^2 - \frac{33}{4}x + 1}$

$P(0)=1$ ✓ $P(4)=0$ ✓
$P(1)=-2$ ✓
$P(3)=4$ ✓

b) $p(x)$ has degree $d=2$ through $\{(1,2),(2,3),(3,5)\}$
Finite Field $GF(7)$

$P(1)\equiv 2 \bmod 7$ $\quad p(2)\equiv 3 \bmod 7$ $\quad p(3)\equiv 5 \bmod 7$

Lagrange Interpolation:

$2^{-1}=4$

$$\Delta_1(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{(x-2)(x-3)}{2} = 4(x^2-5x+6) \pmod 7$$
$$= 4x^2+1x+3 \pmod 7$$

$-1^{-1}=6^{-1}=6$

$$\Delta_2(x) = \frac{(x-1)(x-3)}{(2-1)(2-3)} = \frac{x^2-4x+3}{-1} = 6(x^2+3x+3) \bmod 7$$
$$= 6x^2+4x+4 \bmod 7$$

$$\Delta_3(x) = \frac{(x-1)(x-2)}{(3-1)(3-2)} = \frac{x^2-3x+2}{2} = 4(x^2+4x+2) \bmod 7$$
$$= 4x^2+2x+1 \bmod 7$$

$$P(x) = \sum_1^3 y_i\Delta_i(x) = 2(4x^2+x+3)+3(6x^2+4x+4)+5(4x^2+2x+1)$$
$$= x^2+2x+6 + 4x^2+5x+5+6x^2+3x+5 \bmod 7$$
$$= 11x^2+10x+16 \pmod 7$$
$$\equiv \boxed{4x^2+3x+2 \bmod 7}$$

Check: $P(1) = 4+3+2 = 9 \equiv 2 \bmod 7$ ✓
$P(2) = 16+6+2 = 24 \equiv 3 \bmod 7$ ✓
$P(3) = 36+9+2 = 47 \equiv 5 \bmod 7$ ✓

Problem 4

Assume we have a helper function that divides polynomials using normal long division, so it returns a quotient polynomial but not the remainder polynomial (This is equivalent to a floor division function on integers). Also assume degree(A(x)) $\geq$ degree(B(

a) GCD(A(x), B(x)):

```
    if B(x) == 0:
        return A(x)
    else:
        return GCD(B(x), A(x) - [divide(A(x), B(x)) · B(x)])
```

$$\underbrace{A(x) - [\text{divide}(A(x), B(x)) \cdot B(x)]}_{\text{remainder}}$$

b) $P(x) = x^4 - 1 \quad Q(x) = x^3 + x^2$

$x^3+x^2 \overline{)\, x^4 - 1}$: $x - 1$ r $x^2 - 1$

Using GCD on $P(x)$ & $Q(x)$

$GCD(P(x), Q(x)) = GCD(x^4 - 1, x^3 + x^2)$

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

$= GCD(x^2 - 1, x + 1)$

$= GCD(x + 1, 0)$

$= x + 1 \neq 1.$

$x^2 - 1 \overline{)\, x^3 + x^2}$: $x + 1$ r $x + 1$

$x^3 - x$

$x^2 + x$

$x^2 - 1$

$x + 1$

$x + 1 \overline{)\, x^2 - 1}$: $x - 1$ r 0

$x^2 + x$

$-x - 1$

$-x - 1$

The GCD of P(x) and Q(x) is x+1 (so x+1 divides both without remainder). Since the GCD $\neq 1$, we know P(x) has no multiplicative inverse mod Q(x) and Q(x) has no multiplicative inverse mod P(x). In other words, there is no polynomial that we can multiply P(x) by such that the product is 1 more than Q(x) times some other polynomial, and vice versa.

c) We can do this with an EGCD algorithm for polynomials:

```
EGCD(P(x), Q(x)):
    if Q(x) == 0:
        return (P(x), 1, 0)
    else:
        (D(x), A(x), B(x)) = EGCD(Q(x), P(x) - divide(P(x), Q(x)) · Q(x))
        return (D(x), B(x), A(x) - divide(P(x), Q(x)) B(x))
```

$EGCD(P(x), Q(x)) = EGCD(x^4-1, x^3+x^2)$

$(D, A, B) = (x+1, 1, -x-1)$

return $(x+1, -x-1, 1-(x-1)(-x-1))$

$EGCD(x^3+x^2, x^2-1)$

$(D, A, B) = (x+1, 0, 1)$

return $(x+1, 1, 0-(x+1)1)$

$EGCD(x^2-1, x+1)$

$(D, A, B) = (x+1, 1, 0)$

return $(x+1, 0, 1-(x-1)0)$

$EGCD(x+1, 0) \longrightarrow (x+1, 1, 0)$

$A(x) = -x-1 \quad B(x) = 1-(x^2 \cancel{-x} \cancel{+x} + 1) = x^2 \qquad D(x) = x+1$

$A(x)P(x) + B(x)Q(x)$

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

$\cancel{-x^5} + x \cancel{-x^4} + 1 \cancel{+x^5} \cancel{+x^4}$

$= x+1 = D(x)$ ✓

$\boxed{\text{So } A(x) = -x-1 \quad B(x) = x^2 \text{ and } A(x)P(x) + B(x)Q(x) = x+1}$

Problem 5

Theorem: For every prime p, every polynomial over $GF(p)$ (including degree $\geq p$) is equivalent to a polynomial of degree at most $p-1$.

a) Fermat's Little Theorem: $a^{p-1} \equiv 1 \bmod p$ for all p prime

$a^p \equiv a \bmod p$

Degree p: $x^p = x^{p-1}x^1 \equiv 1x^1 \bmod p \equiv x \bmod p$.

So a degree p is really just degree 1.

$D = p+1$: $x^{p+1} \equiv x^{p-1}x^2 \equiv x^2 \bmod p$

$p+1 \longrightarrow 2$

$D = p+2 \longrightarrow 3$

Fermat's little theorem let's us reduce any term with degree greater than $p-1$. For any degree d, x^d can be reduced to $x^{d \bmod p-1}$. Since $d \bmod p-1$ is at most $p-1$, all polynomials have to be degree of at most $p-1$.

b) We know any polynomial of degree d needs $d+1$ points to be uniquely determined. So a polynomial in $GF(p)$ of degree d needs $d+1$ unique points to determine the polynomial, even if $d > p$. This means we have pairs $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$ which are needed to uniquely identify our polynomial. But we know that in a mod p universe, there are only $p-1$ numbers less than p that are unique mod p, meaning that there are $p-1$ congruence classes. So if $d > p$, then there must be $d-p+1$ x_i's that are in a congruence class of some other x_i that is less than p. Hence there are really only $p-1$ unique x_i values even for $d > p$, and so there are at most $p-1$ unique ordered pairs. From Lagrange interpolation we know that these $p-1$ points uniquely determine a polynomial. So the polynomial with $d > p$ must be the same as the polynomial of degree $p-1$ at all $x_1, \ldots x_{d+1}$ points, and thus we have proven the claim.

Problem 6

Linear Congruential Generator: modulus m, constants a, b, seed x_0

$X_{t+1} = \text{mod}(ax_t + b, m)$

$m = 2^{31} - 1 \longrightarrow m$ is prime. $X_0 = X_0$

$X_1 = ax_0 + b \mod m$

$X_2 = a x_1 + b \mod m$

$X_3 = ax_2 + b \mod m$

$X_4 = ax_3 + b \mod m$

$X_5 = aX_4 + b \mod m$

$X_6 = aX_5 + b \mod m$

$X_7 = aX_6 + b \mod m$

$X_8 = aX_7 + b \mod m$

$X_9 = aX_8 + b \mod m$

We can predict all the values $X_5 \ldots X_9$, as long as we figure out what "a" and "b" are. Given the modulus m and X_0, X_1, X_2, X_3, X_4, this is all we need to solve the system of equations for a & b.

$$X_1 = aX_0 + b \mod m$$
$$\Rightarrow X_1 - aX_0 \equiv b \mod m$$
$$X_2 = aX_1 + b \mod m$$
$$\Rightarrow X_2 - aX_1 \equiv b \mod m$$
$$\Rightarrow X_1 - aX_0 \equiv X_2 - aX_1 \pmod{m}$$
$$\boxed{a = \frac{(X_1 - X_2)}{(X_0 - X_1)}}$$

$$b \equiv X_1 - aX_0 \equiv X_1 - \frac{X_0(X_1 - X_2)}{X_0 - X_1}$$
$$\equiv \frac{\cancel{X_1X_0} - X_1^2 - \cancel{X_0X_1} + X_0X_2}{X_0 - X_1}$$
$$\boxed{b \equiv \frac{X_0X_2 - X_1^2}{X_0 - X_1}}$$

So given X_5, we can find X_6, then X_7, all the way to X_9.

Problem 7

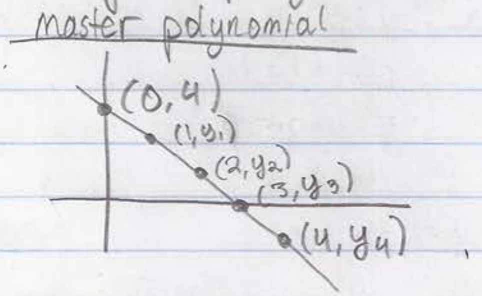
Secret Sharing Rules:

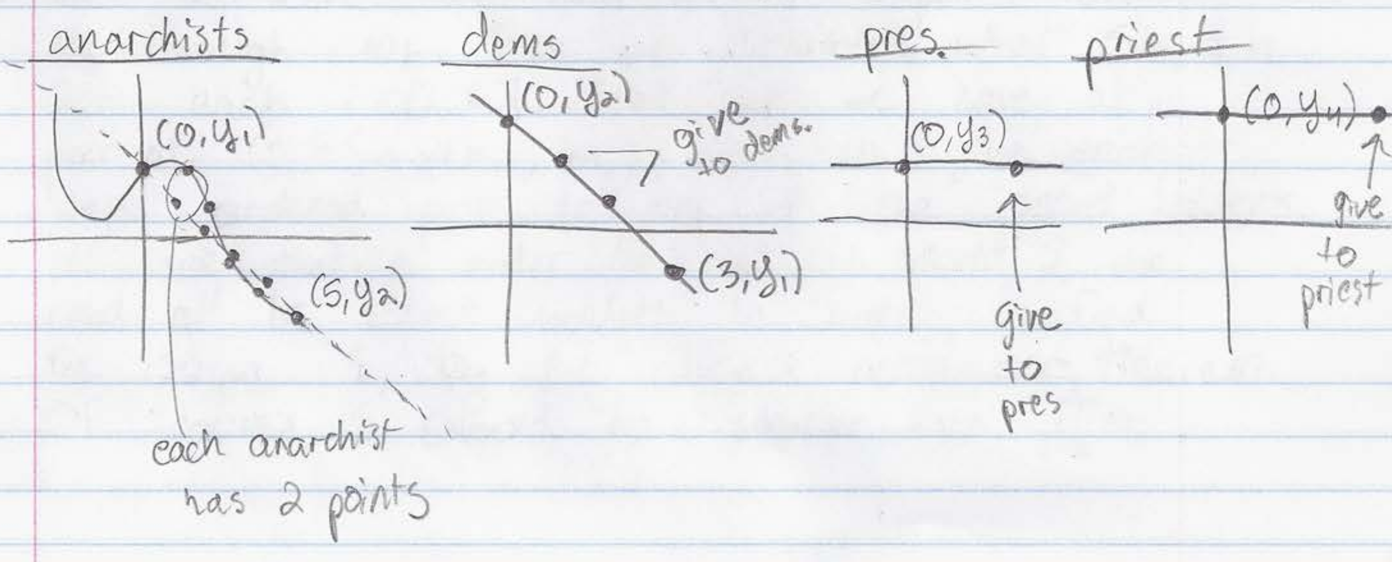
1. The Republic consists of four anarchists, two democrats, the elected President, and the High Priest.
2. Making a move requires a minimum amount of representatives, otherwise the secret instructions are unknown to everyone.
3. If only representatives from one faction agree, the instructions remain secret.
4. If all the represenatives of one faction plus at least one other agrees, the secret instructions are determined

a) Each group has a group secret, $S=4$, that can only be discoved when all the members in a group agree within themselves. We can have each group have its own group secret S_1, S_2, S_3, S_4, but simplicity we will have them all equal 4 (And this is not necessarily the secret instructions). We can just use the normal polynomial secret sharing scheme, adjusting for the number of members in each faction. For the group of anarchists, with four members, we need a polynomial of degree 3. This polynomial can be such that $P_3(0) = S = 4$. We share 4 different ordered pairs on this polynomial (say $(x_1, y_1) \ldots (x_4, y_4)$) and give one to each anarchist, so all 4 of them will need to "agree" in order to find the secret. By "agree", I mean they decide to share their ordered pairs with each other. For the president and priest, we give them a degree zero polynomial $P(x) = 4$, so that when they decide to act independently they can come up with $S=4$ knowing their only ordered pair $(x, 4)$ for any x. The two democrats get a 1 degree polynomial that passes through $(0, 4)$, each of them get a unique polynomial on that line. For any of these factions, as long as they agree within themselves, they can find $S=4$.

b) Once we ensure the factions agree within themselves, we can have a seperate polynomial to get them to agree amongst each other with at least 2 factions. We choose a 1 degree polynomial that passes through $(0, S_{all})$, where S_{all} is the secret that can only be discovered when at least 2 factions agree. Then we find 4 other ordered pairs on this line, and distribute one to each faction. Now if any two factions "agree", they can share their ordered pairs with eachother, and if at least two factions agree then they will have enough points to determine the unique 1 degree polynomial that contains S_{all}.

c) Combining (a) and (b), we can devise a scheme that sticks to the rules. Lets have our secret instructions be $s=4$. Now we choose a 1 degree polynomial with $(0,4)$ as a point. We can then choose 4 additional ordered pairs (i, y_i) for $i \in [1,4]$. Now we will create 4 more additional polynomials such that each polynomial for each group has a point that passes through $(0, y_i)$ for each group i. If group $i=1$ is the anarchists, then they get a 3 degree polynomial, group $i=2$ has a degree 1 polynomial for the democrats, and so on as in part a. Now each group knows its own i index, but they can only figure out their y_i by agreeing within themselves, as described in part a (anarchists share 4 ordered pairs, democrats share 2, etc). Thus once any two factions agree within themselves, they can find 2 points (i, y_i) that are unique and can be used to interpolate for the 1 degree polynomial that passes through $(0, s=4)$. Now we can modify this so that we don't have to have 2 fully agreeing factions, but just 1 faction and 1 other member. We will have it so that the anarchist's y intercept y_1 is also at the point $(3, y_1)$ on the democrats 1 degree polynomial. So if all anarchists agree, and at least 1 democrat agree, they can take $(3, y_1)$ and the democrat's ordered pair to find the democrats group secret y_2. Hence they know $(1, y_1)$ and $(2, y_2)$ on the 1 degree polynomial through $(0, S=4)$. If all the anarchists agree and at least the president or the priest agree, the situation is just part (b). Now for each of the anarchists, give them an additional point (unique) that passes through $(0, y_1)$ and $(5, y_2)$. If all of the democrats agree to find y_2, and at least 1 anarchist wants to share their unique cross faction point to short circuit the other anarchists and find y_1, then they can find the 1 degree polynomial through $(0, S)$.





We can do something similar for when the president or priest want to act and only need one anarchist or 1 democrat. We can give each anarchist a 3rd and 4th point that give the line through $(0, y_1)$ and $(6, y_3)$ and $(7, y_4)$, and each democrat a 2nd and 3rd point through $(4, y_3)$ and $(5, y_4)$ respectively. That way we can always find the line through $(0, s)$.

Problem 8

A polynomial of degree 9 is uniquely determined by 10 points. If we send 25 points, we can still discover the first 10 points (assuming the message is encoded for $x = 1, \ldots, 10$) as long as we get any 10 points of the 25 we sent. So we can handle $25 - 10 = \boxed{15 \text{ erasures}}$ and still have enough points to determine the unique 9 degree polynomial needed to decrypt the message.

Problem 9

Question: Using the Chinese remainder theorem, devise a secret sharing sheme. Describe how to partition the secret into shares, and how many shares are needed to rediscover the secret. What algorithm can be used to find the secret? Compare this to polynomials and error correcting.

Solution:

The Chinese remainder theorem says that given a sequence of coprime numbers $m_1, \ldots, m_k$, there is an x that solves $x \equiv a_1 \bmod m_1, \ldots, x \equiv a_k \bmod m_k$ for any choices of $a_1, \ldots, a_k$.

Scheme - We will have a secret S that we distribute between k secret holders. Before we share the secret, we choose k coprime numbers m_1 through m_k. Then we determine what $S \bmod m_i$ for each $i \in [1, k]$. Now that we have a pair of $(S_i = S \bmod m_i, m_i)$, we can give each of these ordered pairs to one of the secret holders. We see that in order to find the secret S, we need all k secret holders in order to find the unique S, by the chinese remainder theorem. Of course, S should be smaller than $\prod_{i=1}^{k} m_i$.

Algorithm to discover secret: we can just use the normal algorithm for solving the chinese remainder system of equations. For each i, m_i and $(\prod_{i}^{k} m_i)/m_i$ are coprime. Using EGCD, we can find a_i and b_i such that

$$a_i m_i + \frac{(\prod_{i}^{k} m_i)}{m_i} b_i = 1$$

Now call $\frac{(\prod_{i}^{k} m_i)}{m_i} b_i = e_i$. Then $\boxed{x = \sum_{i=1}^{k} s_i e_i}$.

This just says that x is in the congruence class of each mod m_i that we have.

Extension: Like the polynomial secret sharing scheme, each secret holder has a ordered pair (s_i, m_i) that when all k holders are together determine a unique value. However, any less than k we can never recover the secret, unlike the polynomial scheme, where the number of secret holders and the shares needed are independendent. We can't just find extra ordered pairs that don't change the secret. If we wanted to have any more secret sharers, then we need to remake our secret S because each ordered pair has its own m_i, which changes the solution x to the system of equations. Because of this result, we actually can't come up with an erasure error correction algorithm using the chinese remainder theorem.