Today

1. Deterministic Factorization over \( \mathbb{F}_p^k \)

2. Factorization of Bivariate Polynomials.

---

Deterministic Factorization:

Key idea: to factor \( f = f_1 \cdot f_2 \) deg \( \alpha \).

- \( \exists \) non-trivial poly \( g \) s.t.
  \[ g(x)^p - g(x) = 0 \pmod{f} \]

- \( g(x)^p - g(x) = \prod_{\alpha \in \mathbb{F}_p} (g(x) - \alpha) \)

helps factor \( f \)

Can find such \( g \) efficiently by linear algebra.
I. Existence of $g$.

**Defn:** $g$ non-trivial if $0 < \deg g < \deg f$.

1. Exists trivial $g$

   e.g. $g(x) = \alpha \in \mathbb{F}_p$

2. Sufficient to have

   $$g(x)^p - g(x) = 0 \mod f_1$$
   $$g(x)^p - g(x) = 0 \mod f_2$$

3. Now use

   $$g(x) = \alpha \mod f_1$$
   $$g(x) = \beta \mod f_2$$

   $g \in \mathbb{F}_2$ since $g^p = g$ only for $g = \alpha \in \mathbb{F}_p$

   $\deg g < \deg f$ (else use $g(\mod f)$)
III. Finding $g$

- **Idea:** Should be easy since set of all (trivial + non-trivial) solutions form $\mathbb{F}_p^*$ - vector space.

$g, h$ satisfy

\[ g^p - g = 0 \mod f \]
\[ h^p - h = 0 \mod f \]

\[ (g+h)^p - (g+h) = 0 \mod f \]

- Can we find the constraint explicitly over $\mathbb{F}_p^*$?
Representations of $\overline{\mathbb{F}}_q = \mathbb{F}_p^t$?

- Represent by $t$ linearly independent $\alpha_i$:
  $$\alpha_1, \ldots, \alpha_t \in \overline{\mathbb{F}}_q$$

- Along with multiplication identities:
  $$\alpha_i \cdot \alpha_j = \sum_{i,j,k} c_{ijk} \alpha_k \quad c_{ijk} \in \mathbb{F}_p$$

- $g = ?$
  $$g(x) = \sum_{i=0}^{2d-1} \left( \sum_{j=1}^{t} c_{ij} \alpha_j \right) x^i$$
  $$c_{ij} \in \mathbb{F}_p$$

- $g^p = ?$
  $$g(x)^p = \sum_{i=0}^{2d-1} \left( \sum_{j=1}^{t} c_{ij} \alpha_j^p \right) x^i$$

- Reducing $x^p \pmod{f}$ & $\alpha_j^p \rightarrow \sum_{i,k}^\prime e_{ijk} \alpha_k$ are linear maps... can be computed explicitly.
Coefficient of $x^l$ in $g' - g \pmod{\ell}$
is linear function of $C_{ij}$
can be computed efficiently;

(helps to precompute;

$$\alpha_i = \sum_j S_{ij} \alpha_j \quad S_{ij} \in \mathbb{F}_p$$

$$X^e = \sum_{i=0}^{2d-1} \sum_{j=0}^{2d-1} P_{ij} f_j x^i$$

$$p_{ij} \in \mathbb{F}_q$$

where $f = \sum f_i x^i$)

Thus $g$ can be solved by

solving linear system over $\mathbb{F}_p$
II. Find Factorization Algorithm

Step 1: Find non-trivial \( g \) s.t.
\[
g^p - g = 0 \pmod{f}
\]

Step 2: for \( \alpha \in \mathbb{F}_p^* \)
if \( \text{gcd}(f, g - \alpha) = \text{non-trivial} \)
report \( \left( \frac{\text{gcd}(f, g - \alpha)}{\text{gcd}} \right) \).

Claim: \( f \mid g^p - g \Rightarrow \exists \alpha \in \mathbb{F}_p^* \)
\[\text{s.t. } \text{gcd}(f, g - \alpha) \text{ is non-trivial}\]

Proof: obvious
Upcoming Lectures

- Factoring Bivariate Polynomials
- Factoring Rational Polynomials

Common Theme

Input: Polynomial \( f \in R[x] \)

\( (R = \mathbb{F}[y] \text{ or } R = \mathbb{Z}) \)

Plan:

1. Find ideal \( I \in R \)
2. Perturb \( f \)
3. Factor \( f \pmod{I} \) [hopefully easy]
4. Hensel Lifting
   
   Factor \( f \pmod{I^\ell} \) for large \( \ell \)
5. "Jump" to actual factorization.
Details:

1. The ideal: \( I = (y) \) if \( R = \mathbb{F}[y] \)
   \[ = (p) \text{ if } R = \mathbb{Z} \]
   \[ \uparrow \text{prime} \]

Good News: In both cases easy to factor in \( R[x]/I \)

Aside: \( R/I \) the "quotient" ring:

- Always well defined;
- Elements of \( R/I = a + I, a \in R \)
- Sum/product as natural
  \[(a + I) + (b + I) = (a + b) + I \]
  \[(a + I) \cdot (b + I) = ab + I \]

This is what we used to create extension fields "closed under \( R \) mult"
Last step: The jump?

What does it do? Why?

To understand we need to understand what could happen at first step.

Suppose \( f = f_1 \cdot f_2 \cdot f_3 \cdots f_k \) in \( \mathbb{R}[x] \)

1. Can \( f \) have fewer factors in \( \mathbb{R}[x]/I \)?
2. Can \( f \) have more factors in \( \mathbb{R}[x]/I \)?

Answers: YES and YES.

\( \forall j \Rightarrow \) Some \( f_i \) (mod \( I \)) may become constants.

(e.g. \( f_i = \alpha + p \cdot g(x) \))

\( \alpha + y \cdot g(x) \)

But a rare event... will have to prove; prevent by perturbing.
\( f \in \mathbb{F}_p[x, y] \)  
\[ f(x, y) = x^p - x + y \cdot g(x, y) \]

- \( f \) is probably irreducible but factors completely \((\text{mod } y)\).

- **Hensel lifting?**

  \[ f = f_1 \cdot f_2 \cdot \ldots \cdot f_p \pmod{I} \]

  \[ \exists \]

  \[ f = f'_1 \cdot f'_2 \cdot \ldots \cdot f'_p \pmod{I^t} \]

  Will lift whenever conditions are good.

- So need to use \( f'_i \) to find some non-trivial irreducible factor of \( f \).

- Modulo some math
  
  \( \Rightarrow \) linear algebra in \( \mathbb{F}[x, y] \).
  \( \Rightarrow \) lattice reduction in \( \mathbb{Z}[x] \).
Some Math

Why should $f_i$ give info on factors of $f$?

- Suppose $f = g_1 \cdot g_2 \cdot g_3 \cdots g_e$

- $f_1 \cdots f_k$ are (if we're lucky)
  factorizations of $g_1 \cdots g_e \pmod{I}$

- So $f_i$ comes from one of the $g_i$'s
  say $g_i$

What do we know about $g_i$:

- factor of $f$
  - has $f'$ as factor modulo $I^t$
  - has degree $< \deg(f)$
  - coefficients of $g_i$ small if coeff. of $f$ are small.
**Problem:** Given $h \in \mathbb{F}[x,y]$ of deg $D$ find $g \in \mathbb{F}[x,y]$ of deg $d \leq D$ s.t. $\exists \, \tilde{g} \text{ s.t. } g = \tilde{g} \cdot h \pmod{y}$

**Solution:** Linear algebra

Given $\tilde{g}$, $g$ is a linear form in coefficients of $\tilde{g}$.

- Does this really solve the problem?
- Will $g = g$, that we care about?
- Will defer proof, but answer is YES
**Problem:** Given \( h \in \mathbb{Z}[x] \), find \( g \in \mathbb{Z}[x] \) with "small" coefficients such that
\[
\exists \tilde{g} \in \mathbb{Z}[x] \quad \text{s.t.} \\
g = \tilde{g} \cdot h \pmod{N}
\]

**Solution:** "Short vector in lattice problem."

- Set of solutions form a lattice in \( \mathbb{Z}^{d+1} \):
  \((g_i, \tilde{g}_i) \) and \((g_j, \tilde{g}_j) \) are solutions
  \[ (g_i + g_j, \tilde{g}_i + \tilde{g}_j) \] is solution
- if \( h = \sum_i x^i \) and \( g = \sum_i g_i x^i \), then the lattice spanned by columns of

\[
\begin{bmatrix}
  h_0 & 0 & N & 0 \\
  h_1 & h_0 & N & 0 \\
  \vdots & \vdots & \vdots & \vdots \\
  h_r & \cdots & h_0 & N \\
  0 & \cdots & h_r & 0 \\
  \end{bmatrix}
\]
Main Questions: (in lin. algebra / lattice)

- Why does appropriate \( g \) exist?
- If it exists, is it unique, or will all \( g \) exist?

Usual answers

- Solution exists because the irreducible factor we are looking for satisfies all criteria.
- Solution is not unique.
- "Any solution of minimum degree will do."

This needs formalization + proof.
"Uniqueness" Lemmas

Lemma ($\mathbb{F}[y]$): Let $h \in \mathbb{F}[x,y]$ with $\deg(h) \leq 1$.

$(a,\bar{a}) \neq (b,\bar{b})$ be two sets of solutions to $(g,\tilde{g})$ in system below:

\[ g = \tilde{g} \cdot h \pmod{y^t} \]

\[ \deg(g) \leq d \; ; \]

Furthermore let $a$ be solution of smallest $x$ degree. Then, if $t \geq \text{??}$, 

$a \mid b$.

(See, in our case, if $b$ is the solution we desire & $a$ is the solution we find of min. degree, then $a \sim b$.)
Lemma (Z): Let \( h \in \mathbb{Z}[x] \) with \(|\text{coeff.}| \leq M_0 \) \& \( \deg(h) \leq d \).

Let \( (a, \tilde{a}) \) \& \( (b, \tilde{b}) \) be solutions to
\[
g = \tilde{g} \cdot h \mod N
\]
\(|\text{coeff. of } g| \leq M_1 \).

Then if \( \deg_x(a) \) is smallest possible,
\& \( N > N(m_0, m_1) \) then \( a | b \).

Proofs: Need to introduce Resultants
\& 0 bound \text{coeff. if factors}.
**Boring Part: Bounding Coefficients**

**Lemma:** Let \( a = \sum a_i x^i \) divide \( b = \sum b_i x^i \). Then if \( 1 |b| < 2^n \), \( 1 |a| < 2^{n+\text{poly}(1)} \) \( [a_i, b_i \in \mathbb{Z}] \)

**Sublemma 1:** All complex roots of \( b = \sum b_i x^i \) bounded by \( B = \max_i \{ 1 + |b_i| \} \)

**Proof:** \( b_n B^n \geq B^n > \max_i |b_i| \cdot \sum_{i=0}^{n-1} b_i \geq |b_i| B \), so \( B \) can't be a root.

**Sublemma 2:** if all complex roots of \( a = \sum a_i x^i \) are bounded by \( B \), then \( |a_i| \leq 2B^i m \)

**Proof:** follows since coefficients are the symmetric polynomials in roots, mult. by \( a_m \)
Back to Uniqueness Lemmas

How to prove $a | b$?

- Actually we'll try to prove $\gcd(a, b) \neq \text{non-trivial}$

- take the case where $a, b \in \mathbb{F}[x, y]$

- view them as elements of $\mathbb{F}(y)[x]$.

- if they don't have a common factor (of positive degree in $x$) then

  $\exists u, v \in \mathbb{F}(y)[x]$ s.t.

  $u \cdot a + v \cdot b = 1$

- clearing denominators we get

  $\exists \overline{u}, \overline{v} \in \mathbb{F}[x, y] \land r \in \mathbb{F}[y]$

  $a + \overline{u} \cdot a + \overline{v} \cdot b = r$

- degree of $r = ?$
### Resultants!

- Low-degree polynomial in ideal generated by $a, b$
- Specifically if $a, b$ relatively prime in $\mathbb{F}_p[x, y]$, then $R \in \mathbb{F}[y]$ of degree $\deg(a) \cdot \deg(b)$

**Definition:** $a, b \in R[x]$ of degree $k, \ell$, respectively. Let $a = \sum a_i x^i$ and $b = \sum b_i x^i$.

Let

$$M(a, b) = \begin{bmatrix} a_0 & 0 & b_0 \\ a_1 & a_0 & b_1 \\ \vdots & \vdots & \vdots \\ a_k & a_{k-1} & b_k \end{bmatrix}$$

Then $\text{Res}_x(a, b) \triangleq \text{determinant}(M(a, b))$

**Note:** $\text{Res}_x(a, b) \in R$
Motivation

- a and b have common factor \( g \in \mathbb{R}[x] \) of positive degree in \( x \) \( \iff \) there exists a solution to \( u, v \in \mathbb{R}[x] \)

\[ a \cdot u + b \cdot v = 0 \]  

(2) \deg(u) < \deg(b) \quad \text{and} \quad \deg(v) < \deg(a)

Writing \( u = \sum_{j=0}^{l-1} u_j x^j \) and \( v = \sum_{j=0}^{k-1} v_j x^j \) and solving for the unknowns, we are solving

\[
M(a, b) \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_{l-1} \\ v_0 \\ v_1 \\ \vdots \\ v_{k-1} \end{bmatrix} = \begin{bmatrix} 0 \end{bmatrix} \quad \text{for a non-zero solution.}
\]

A solution exists iff \( \text{Res}(a, b) = 0 \).
Properties of resultant

1. \( \text{Res}(a,b) \in \text{Ideal}(a, b) \)

**Claim 1:** \( \forall M \in \mathbb{R}^{n \times n}, \) the vector \( \begin{pmatrix} \text{Det}(M) \\ 0 \\ \vdots \\ 0 \end{pmatrix} \) is in the column span of \( M \).

**Proof:** Can do column operations on \( M \) to convert it to \( \begin{bmatrix} g_1 \\ g_2 \\ 0 \\ \vdots \\ g_n \end{bmatrix} \) s.t.

\[
\text{det}(M) = \prod g_i.
\]

Can now generate \( \begin{pmatrix} \text{det}(M) \\ 0 \\ \vdots \\ 0 \end{pmatrix} \) from above by taking some \( \mathbb{R} \)-linear combinations.

\[\text{Claim 1: } \Rightarrow \text{ 1) immediately}\]
2) \( \text{Res}(a, b) \) is poly in coeff of \( a, b \) of 
\[ \text{deg} \leq \text{deg}(a) + \text{deg}(b) \]

2') \( a, b \in F[x, y] \) with \( \text{deg}(a) = k, \text{deg}(b) = l \) 
\[ \Rightarrow \text{Res}_x(a, b) \) is poly of \( \text{deg} k.l \) in \( y \)

Proof: Careful counting.
\[ \text{deg} \left( M(a, b) \right)_{i,j} \leq k - i + j \text{ if } j \leq l \leq j - i \text{ if } j > l \]

Thus a permutations \( \sigma \)
\[ \text{deg} \left( \prod_{j} M(a, b)_{\sigma(j), j} \right) \leq kl \]

Lemma: \( a, b \in F[x, y] \) of \( \text{deg} \leq k, l \) resp. with no common factor of degree > 0
in \( x \) \( \Rightarrow \exists R(y) \) of \( \text{deg} \leq k.l \) in \( I(a, b) \)

Proof: Resultant.
**Applications of Resultants**

**Bezout's Theorem (weak form, in the plane)**

\( a, b \in \mathbb{F}[x,y] \) have \( > k \cdot l \) common points

\[ \implies a, b \text{ have common factor.} \]

**Proof:** Let \( t = k \cdot l + 1 \) & let

\( (\alpha_1, \beta_1), \ldots, (\alpha_t, \beta_t) \in \mathbb{F} \times \mathbb{F} \) be

\( t \) common zeroes.

- By affine-coordinate transform, can assume \( \beta_i \)'s are all distinct.
  (work over \( \overline{\mathbb{F}} \) if needed)

- Every poly in \( I(a,b) \) vanishes at

  \( (\alpha_1, \beta_1), \ldots, (\alpha_t, \beta_t) \).

- If no common factor, \( \text{Res}(a,b) = R(y) \) is zero at \( \beta_1, \ldots, \beta_t \)

- Contradicts \( \text{deg}(R) < t \). \( \Box \)
Application 2: Repeated factors

Lemma: If \( f \in \mathbb{F}[x,y] \) is square-free (no \( q \) s.t. \( q^2 \mid f \))

then \( \left| \{ \beta \in \mathbb{F} \mid f(\cdot,\beta) \text{ has square factor} \} \right| \leq d^2 \)

Proof: \( f \) is square-free \( \Leftrightarrow \) \( (f, f') \) have no common factor.

\( \Delta = \text{Disc}(f) \equiv \text{Res}_x (f, f') \neq 0 \)

\( \Delta \in \mathbb{F}[y] \) of deg \( \leq d^2 \)

Similarly \( f_\beta = f(\cdot,\beta) \) is square-free iff \( \text{Disc}(f_\beta) \neq 0 \)

But \( \text{Disc}(f_\beta) = \Delta(\beta) \)

\[ \Box \]
**Back To Uniqueness Lemma (Page 15)**

**Lemma:** $(a, \overline{a}), (b, \overline{b})$ satisfy

\[
a = \overline{a} \cdot h \pmod{y^t}; \\
b = \overline{b} \cdot h \pmod{y^t}; \\
\deg(a, b) \leq d; \\
\]

\[\Rightarrow a \mid b \]

\[\Rightarrow t > d^2 \]

**Proof:** Assume $a \nmid b$. Then $\exists u, v \in \mathbb{F}[x, y]
\begin{align*}
\text{s.t. } & a \cdot u + b \cdot v = R = \text{Res}_x(a, b) \in \mathbb{F}[y]/0 \\
\Rightarrow & \overline{a} \cdot h \cdot u + \overline{b} \cdot h \cdot v = R = 0 \pmod{y^t} \\
\text{But } & R \text{ is non-zero } \& \text{ of degree } \leq d^2 < t \\
\Rightarrow & R \neq 0 \pmod{y^t}
\end{align*}
\]

\[\mathbb{Z}[x] \text{ version similar; argue about size of } R \text{ as opposed to degree } t.\]
Hensel Lifting

Will describe process first; see what it needs to work & will get lemma later. Structure of lemma below

"Lemma": let $I \subseteq R$ be an ideal.

- Let $f, g, h \in R[x]$ satisfy $f = g \cdot h \pmod{I}$

- Then under some conditions on $g, h$, the factorization can be lifted, i.e.,
  $$\exists \tilde{g}, \tilde{h} \quad \tilde{g} = g \pmod{I} \land \tilde{h} = h \pmod{I}$$
  $$\implies f = \tilde{g} \cdot \tilde{h} \pmod{I^2}.$$  

- Such $\tilde{g}, \tilde{h}$ can be found efficiently.

- They are unique in some sense?
Suppose \( f = q \cdot h - r \) \( \quad r \in I \)

\[ g = g + g \cdot r \quad , \quad h = h + h \cdot r , \]

\[ \tilde{g} \cdot \tilde{h} = g \cdot h + r ( g \cdot h + h g ) + r^2 ( g , h ) \]

\[ \quad = f + r ( 1 + g \cdot h + h g ) + r^2 ( g , h ) \]

\[ \quad = f + r ( 1 + g \cdot h + h g ) \quad ( \text{mod} \quad I^2 ) \]

Would like to pick \( g_1 \) s.t.

\[ g_1 = - ( h_1 g + 1 ) \cdot h^{-1} \quad ( \text{mod} \quad I ) \]

Does \( h \) have inverse \( ( \text{mod} \quad I ) \)?

Will make it a precondition, but now will also be part condition. \( \tilde{h} \) will be invertible.
Uniqueness of lifts?

- Can't be unique! I can add arbitrary elements of \( I^2 \) to \( \tilde{g}, \tilde{h} \).

- Also if \( \tilde{g}, \tilde{h} \) are solutions, so are \( \tilde{g}(1+u), \tilde{h}(1-u) \) for \( u \in I \).

- Essentially above are the only things that can happen.
**Hensel Lifting Theorem**

- \(R\) commutative ring, \(I \subseteq R\) ideal

- \(f, g, h \in R[x]\) s.t. \(f = g \cdot h \pmod{I}\)

- \(g, h\) relatively prime, i.e.,
  
  \[\exists a, b \in R[x] \quad \text{s.t.} \quad a \cdot g + b \cdot h = 1 \pmod{I}\]

Then

- \(\exists \tilde{g}, \tilde{h}, \tilde{a}, \tilde{b}, \quad \tilde{g} = g \pmod{I}, \tilde{h} = h \pmod{I}\)

  \[\text{s.t.} \quad f = \tilde{g} \cdot \tilde{h} \pmod{I^2}\]

  \[\tilde{a} \cdot \tilde{g} + \tilde{b} \cdot \tilde{h} = 1 \pmod{I^2}\]

- \(\tilde{g}, \tilde{h}\) are essentially unique, i.e., if
  
  \(\bar{g}, \bar{h} = f \pmod{I^2} \land g = g \pmod{I}\)

  \(h = h \pmod{I}\)

then \(\exists u \in I\) s.t.

\[g = \tilde{g}(1 + u) \quad \text{and} \quad h = \tilde{h}(1 - u)\]

[Proof = Exercise]
Bivariate Factorization

Input: $f \in R[x,y]$ of deg $d$

Goal: find non-trivial split of $f$.

Alg: 0. If $\gcd(f,f')$ non-trivial, report $\gcd$ & stop.

1. Pick $\beta \in R$ at random $\alpha$

   factor $f_{\beta} = f(x,y+\beta)$ instead

2. Factor $f_{\beta} = g_{\beta} \cdot h_{\beta} \pmod{y}$

   s.t. $g_{\beta}, h_{\beta}$ relatively prime

   if can't find such split., abort.

3. Lift $\log t = \log d^2$ times to get

   $f_{\beta} = \bar{g}_{\beta} \cdot \bar{h}_{\beta} \pmod{y^t}$

4. Jump from $\bar{g}_{\beta}$ to $g_0$, irreducible

   s.t. $g_0 \mid f_{\beta}$