Math Notes

John L. Manferdelli

These notes were written for my personal use, partly to learn tex.
They are clearly not written for third parties (second parties either)
and may be incomplete, inaccurate or even incoherent.
I disclaim any and all liablity for errors, omissions, inaccuracy,
infringement, or any other liability based on another party's
use, duplication, distribution or reliance on these materials.
However, you are welcome to use them at your own risk.

Corrections are welcome. Please send them to
John Manferdelli,
285 Douglass St, San Francisco, CA 94114, or
JohnManferdelli@hotmail.com.
jlmucbmath@gmail.com.

Last modified: 30 October 2021 16:13

Chapter 1

Math

1.1 Number Theory, Inequalities and Combinatorics

1.1.1 Basic Number Theory

Theorem: π is irrational.

Proof (Niven): Assume to the contrary that $\pi = \frac{a}{b}, a, b \in \mathbb{Z}$. Define $f_n(x) = \frac{x^n(a-bx)^n}{n!}$ and $F_n(x) = f_n(x) - f_n^{(2)}(x) + f_n^{(4)}(x) - \ldots\ldots + (-1)^n f_n^{(2n)}(x)$. If $x = 0$ or π, $f_n^{(i)}(x) \in \mathbb{Z}, \forall i$ so $F_n(0), F_n(\pi) \in \mathbb{Z}$. $(F'(x)sin(x) - F(x)cos(x))' = (F''(x) + F(x))sin(x) = f_n(x)sin(x)$ so $\int_0^\pi f_n(x)sin(x)dx = F_n(\pi) - F_n(0) \in \mathbb{Z}$. Now suppose, $0 < x < \pi = \frac{a}{b}$. Then $0 < bx < a$, $0 < a - bx < a$, $0 < (a - bx)x < ax < a\pi$ and thus $0 < x^n(a - bx)^n < a^n\pi^n$, $0 < f_n(x)sin(x) \leq f_n(x) = \frac{x^n(a-bx)^n}{n!} < \frac{a^n\pi^n}{n!}$. Pick n large enough that $\frac{\pi^n a^n}{n!} < \frac{1}{\pi}$ then $0 < \int_0^\pi f_n(x)sin(x)dx < 1$. But $\int_0^\pi f_n(x)sin(x)dx = F_n(\pi) - F_n(0) \in \mathbb{Z}$ and this contradiction proves the result.

Theorem: e is transcendental.

Proof: If $f(x)$ is a polynomial of degree r, set $F(x) = f(x) + f'(x) \ldots + f^{(r)}(x)$. Then $F(i) - e^i F(0) = -ie^{i(1-\theta_i)} f(i\theta_i) = \epsilon_i$. Suppose e satisfies $g(e) = c_n e^n + \ldots + c_0 = 0$. Then $c_n F(n) + \ldots + c_0 F(0) = c_1\epsilon_1 + c_2\epsilon_2 + \ldots + c_n\epsilon_n$. Put $f(x) = \frac{1}{(p-1)!}x^{p-1}(1-x)^p(2-x)^p \ldots (n-x)^p$. $p \mid F(i), i > 0$ but $p \nmid F(0)$. So, $c_n F(n) + \ldots + c_0 F(0)$ is an integer not divisible by p but $c_n F(n) + \ldots + c_0 F(0) = c_1\epsilon_1 + c_2\epsilon_2 + \ldots + c_n\epsilon_n$. Now, let $p \to \infty$.

Wilson: $(p-1)! = (-1) \pmod p$.

Proof: There are only two solutions to $x^2 = 1 \pmod p$, namely, ± 1. Thus, if we multiply all non-0 elements of $\mathbb{Z}_p$ together, except for ± 1, each multiplicative element can be paired with its inverse leaving $(1)(-1)$.

Theorem: $\exists x$: $x^2 = -1 \pmod p$ iff $p = 2$ or $p = 1 \pmod 4$.

Proof: $(p-1)! = -1 = (-1)^{\frac{p-1}{2}} \prod_{j \in \{1,2,\ldots,\frac{p-1}{2}\}} j^2 \pmod p$, if $p = 1 \pmod 4$, first factor is 1 and thus $(\prod_{j \in \{1,2,\ldots,\frac{p-1}{2}\}} j)^2 = -1 \pmod p$.

Theorem: If $p = 1 \pmod 4 : \exists a, b : a^2 + b^2 = p$.

Proof: $\exists x : x^2 + 1 = rp$. Set $k = \lfloor \sqrt{p} \rfloor, k \leq \sqrt{p} < k + 1$. Set $f(u, v) = ux + v$; consider $S = \{(u, v) : 0 \leq u \leq k, 0 \leq v \leq k\}$. $|S| = (k + 1)^2 > p$, so $\exists u_1, u_2, v_1, v_2 : f(u_1, v_1) = f(u_2, v_2)$ and $a = u_1 - u_2, b = v_1 - v_2$ then $a + bx = 0 \pmod{p}$. Now $a^2 + b^2 = a^2 + a^2x^2 = 0 \pmod{p}$. $|a| < \sqrt{p}$ and $|b| < \sqrt{p}$ so $0 < a^2 + b^2 < 2p$ and $a^2 + b^2 = p$.

Theorem: If $q \mid (a^2 + b^2)$ and $q = 3 \pmod 4$ then $q \mid a$ and $q \mid b$.

Proof: Suppose $(a, q) = 1$, pick $\overline{a} : a\overline{a} = 1 \pmod q$. $a^2 = -b^2 \pmod q$ so $-1 = (b\overline{a})^2 \pmod q$.

If $n = 2^\alpha \prod_{p=1 \pmod 4} p^\beta \prod_{q=3 \pmod 4} q^\gamma$ then $n = a^2 + b^2$ iff all γ are even.

Proof: Use $(a^2 + b^2)(c^2 + d^2) = (ac - db)^2 + (ad - bc)^2$.

Theorem (representing integers as sums of squares): There are no solutions to $x^2 + y^2 = n$ if $n = 3 \pmod 4$. There are solutions to $x^2 + y^2 = p$, p, prime if $p = 1 \pmod 4$.

Proof: $\exists m, a, b : a^2 + b^2 = mp$ if $p = 1 \pmod 4$; for example, $\exists a : a^2 + 1 = 0 \pmod p$ by Euler's criteria. Note that $(ua + vb)^2 + (va - ub)^2 = (u^2 + v^2)(a^2 + b^2)$. Now apply Fermat's descent, suppose $a^2 + b^2 = mp$. Choose $u = a \pmod m, v = b \pmod m, -\frac{m}{2} \leq u, v \leq \frac{m}{2}$ then $a^2 + b^2 = u^2 + v^2 = 0 \pmod m$. $u^2 + v^2 = mr$ and $(ua + vb)^2 + (va - ub)^2 = m^2rp$. $m \mid (ua + vb)$ and $m \mid (va - ub)$ so $(\frac{ua+vb}{m})^2 + (\frac{va-ub}{m})^2 = rp, r < m$. If a has A divisors $a_1, \ldots, a_A$ with $a_i = 1 \pmod 4$ and B divisors $b_1, \ldots, b_B$ with $b_i = 3 \pmod 4$ then $x^2 + y^2 = n$ has $4(A - B)$ solutions in the integers.

Chinese Remainder Theorem: If $(m_1, m_2) = 1$, for any a, b, there is an n such that $n = a \pmod{m_1}$ and $n = b \pmod{m_2}$. Further, if n' is another such number, $n = n' \pmod{m_1 m_2}$.

Solving Linear Equations over $\mathbb{Z}$: $ax = b \pmod m$ has a solution iff $(a, m) \mid b$. If such a solution exists, there are $\frac{m}{(a,m)}$ solutions.

Theorem: If $(m_1, m_2) = 1$ then $\phi(m_1 m_2) = \phi(m_1)\phi(m_2)$. If $N_f(m)$ is the number of solutions of $f(x) = 0 \pmod m$ and $(m_1, m_2) = 1$ then $N(m_1 m_2) = N(m_1)N(m_2)$.

Proof: Let $x_1, x_2, \ldots, x_j$ be the solutions to $f(x) = 0 \pmod{m_1}$ and $y_1, y_2, \ldots, y_k$ be the solutions to $f(x) = 0 \pmod{m_2}$. By the Chinese remainder theorem there is a unique $z_{i,l} \pmod m$ such that $z_{i,l} = x_i \pmod{m_1}$ and $z_{i,l} = y_l \pmod{m_2}$ for each $1 \leq i \leq j$ and $1 \leq l \leq k$. The $z_{i,l}$ constitute all the solutions to $f(x) = 0 \pmod m$.

Theorem: If $R = R_1 \times R_2 \times \ldots \times R_n$ then $U(R) = U(R_1) \times U(R_2) \times \ldots \times U(R_n)$.

Corollary: If $(m_i, m_j) = 1$ and $m = m_1 m_2 \ldots m_n$ then $\mathbb{Z}/(m) = \mathbb{Z}/(m_1) \times \mathbb{Z}/(m_2) \times \ldots \times \mathbb{Z}/(m_n)$. Applying this to $n = 2^{e_0} {p_1}^{e_1} {p_2}^{e_2} \ldots {p_n}^{e_n}$ we find n has a primitive root iff $n = 2, 4, p^e$. p has $\phi(p - 1)$ primitive roots.

Artin's conjecture: 2 is a primitive root for infinitely many primes. The extended Riemann Hypothesis implies Artin's conjecture.

Lucas' Theorem: If $(a, m) = 1$ and $a^{p-1} = 1 \pmod m$ and $p - 1$ is the smallest such exponent then m is prime.

Definition: For $0 \leq a \leq b \leq n$ with $(a, b) = 1$, the Farey sequence F_n is the ordered list of $\frac{a}{b}$.

$F_3 = \{0, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, 1\}$.

Theorem: If $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \frac{p_3}{q_3}$ are three successive terms of a Farey sequence then $p_1q_1 - p_1q_2 = 1$ and $\frac{p_1+p_3}{q_1+q_3} = \frac{p_2}{q_2}$.

Chevalley's Theorem: Suppose $f \in k[x_1, \ldots, x_n]$, $k = F_q, q = 0 \pmod p$ and $deg(f) = d < n$ then (1) if $f(x) = 0 \pmod p$ has a solution, it has at least two; and (2) if $f(0) = 0$, f has at least one non-trivial solution.

Proof:

Lemma 1: If $u \in \mathbb{Z}, u \geq 0$ and $S(u) = \sum_{x \in k} x^u$ then $S(u) = -1 \pmod p$, if $(q-1) \mid u$ and 0 otherwise.
Proof of lemma: If $u = 0$, $S(0) = q = 0 \pmod p$. If $(q-1) \nmid u, \exists y \in k : y^u \neq 1$, so $S(u) = \sum_{x \in k} x^u = \sum_{x \in k} y^u x^u$ and $S(u) = y^u S(u)$ and thus $(1 - y^u)S(u) = 0$ and $S(u) = 0$. Finally, if $(q-1) \mid u$, $x^u = 1$ if $x \neq 0$ and $x^u = 0$ if $x = 0$; thus $S(u) = q - 1 = -1 \pmod p$.

Put $p(x) = 1 - f(x)^{q-1}$, and let N be the number of zeros of f. $p(x) = 1$ if x is a zero of f and $p(x) = 0$ if x is not a zero of f, so $N = \sum_{x \in k} p(x)$. $p(x)$ is a sum of monomials in n variables and since $deg(p) = d(q-1)$, at least one variable in the monomial appears to a power $< q-1$. By the lemma, the sum over k of each of these monomials is 0 and so $\sum_{x \in k^n} p(x) = 0 \pmod p$ so $N = 0 \pmod p$ and the two assertions follow.

Theorem: Solutions of $f(x) = 0 \pmod p$ are solutions of $(f(x), x^p - x)$. If $deg(f(x)) = n$ with leading coefficient 1 then $f(x)$ has n solutions iff $f(x) \mid (x^p - x)$. If $d \mid (p-1)$ then $x^d = 1 \pmod p$ has d solutions.

Hensel Lemma: Suppose $f(x) \in \mathbb{Z}[x]$. If $f(a) = 0 \pmod{p^j}$ and $f'(a) \neq 0 \pmod p$, there is a unique $t : f(a + tp^j) = 0 \pmod{p^{j+1}}$.

Proof: $f(x + h) = f(x) + hf'(x) +$ terms in h^2 or higher. $f(a) = rp^j$, so $f(a + tp^j) = f(a) + tp^j f'(a) +$ terms in p^{2j} or higher. Thus $f(a + tp^j) = (r + tf'(a))p^j \pmod{p^{j+1}}$. Find $t : r + tf'(a) = 0 \pmod p$. Then $f(a + tp^j) = 0 \pmod{p^{j+1}}$.

Theorem: If $(m, n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$. $\sum_{d|n} \phi(d) = n$. $\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$. $0 = \sum_{d|n} \mu(d)$, if $n > 1$; $\mu(1) = 1$.

Proof: If $r_1, \ldots, r_a$ is a reduced residue set $\pmod m$, $s_1, \ldots, s_b$ is a reduced residue set $\pmod n$ and $x = s_i r_j$ then $(x, mn) = 1$. Further, by the CRT, if $(x, mn) = 1$ then $\exists! i, j : x = r_i \pmod m$ and $x = s_j \pmod n$. This proves the first statement. If $n = p^e$ then $\sum_{d|n} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) + \ldots + \phi(p^e) = 1 + (p-1) + (p^2 - p) + \ldots + (p^e - p^{e-1}) = p^e = n$. Applying the prior result, completes the proof of the second result. If $n = p_1^{e_1} p_2^{e_2} \ldots p_t^{e_t}$, define $\mu(n) = 0$, if $e_j > 1$ for any j, otherwise $\mu(n) = (-1)^t$. μ is multiplicative and the result follows.

Definition: If $n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot \ldots \cdot {p_k}^{\alpha_k}$, define $\mu(n) = (-1)^{\sum_{i=1}^{k} \alpha_i}$.

Moebius Formula: If $f(n)$ is multiplicative and $F(n) = \sum_{d|n} f(d)$ then $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$; if $f(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$ for every $n > 0$ then $F(n) = \sum_{d|n} f(d)$. $\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$.

Proof: $\sum_{d|n} \mu(d) F(\frac{n}{d}) \sum_{d|n} \mu(d) \sum_{\delta | \frac{n}{d}} f(\delta) = \sum_{\delta|n} \sum_{d|\frac{n}{\delta}} \mu(d) f(\delta) = \sum_{\delta|n} f(\delta) \sum_{d|\frac{n}{\delta}} \mu(\delta) = f(n)$.

Theorem: If $(x,n)=1$ then $x^{\phi(n)}=1 \pmod n$. Counterexample to converse (first *Carmichael Number*): 561.

Theorem: The multiplicative group of a finite field is cyclic. $(\frac{a}{p})=a^{\frac{p-1}{2}}$.

Proof: $x^p-x=\prod_{a\in F_p}(x-a)=x\prod_{a\in F_p^*}(x-a)=x(x^{p-1}-1)$. If F_p^* does not have an element of order $m=p-1$ then $\forall x\in F_P^*, x^k=1$ for some $k<m$. But $x^k-1\neq x^m-1$ so F_p^* has an element of order $m=|F_p^*|$ and so the multiplicitive group is cyclic. Let g be a generator for F_p^*, and suppose $a=g^n$. a is a square iff n is even (and $(g^{\frac{n}{2}})^2=a$). In this case, $a^{\frac{p-1}{2}}=((g^{\frac{n}{2}})^2)^{\frac{p-1}{2}}=(g^{\frac{n}{2}})^{p-1}=1$.

Gauss' Lemma: For any odd prime, p with $(a,p)=1$. Consider the integers $a,2a,3a,\ldots,\frac{p-1}{2}a$. If μ is the number of these whose least positive residue modulo p greater than $\frac{p}{2}$, then $(\frac{a}{p})=(-1)^\mu$.

Suppose $r_1,r_2,\ldots,r_\mu$ be the residues that exceed $\frac{p}{2}$ and $s_1,s_2,\ldots,s_\nu$ are the residues that are less than $\frac{p}{2}$. Taken together the set, $s_1,\ldots,s_\nu,(p-r_1),\ldots(p-r_\mu)$ is just $1,2,\ldots,\frac{p-1}{2}$. Thus, $(p-r_1)\ldots(p-r_\mu)s_1s_2\ldots s_\nu=\frac{p-1}{2}!a^{\frac{p-1}{2}}=(-1)^\mu\frac{p-1}{2}!$.

Theorem: If p is an odd prime and $(a,2p)=1$ then $(\frac{a}{p})=(-1)^t$ where $t=\sum_{j=1}^{\frac{p-1}{2}}\lceil\frac{ja}{p}\rceil$ and $(\frac{2}{p})=(-1)^{\frac{p^2-1}{8}}$.

Proof: $\sum_{j=1}^{\frac{p-1}{2}}ja=\sum_{j=1}^{\frac{p-1}{2}}p\lceil\frac{ja}{p}\rceil+\sum_{j=1}^{\mu}r_j+\sum_{j=1}^{\nu}s_j$.

Law of quadratic reciprocity: If p,q are odd primes, $(\frac{p}{q})(\frac{q}{p})=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, $(\frac{2}{p})=(-1)^{\frac{p^2-1}{8}}$.

Proof (Gauss): Let $Dx=g_xp+r_x$. Set $\rho_x=r_x$, if $r_x<\frac{p}{2}$, $\rho_x=r_x-p$, if $r_x>\frac{p}{2}$. Let n be the number of ρ_x that are less than 0. Multiplying $D,2D,3D\ldots\frac{p-1}{2}D$ together, we get: $D^{\frac{p-1}{2}}\frac{p-1}{2}!=(\frac{D}{p})\frac{p-1}{2}!$ and since $D^{\frac{p-1}{2}}\frac{p-1}{2}!=(-1)^n\frac{p-1}{2}!\pmod p$, $D^{\frac{p-1}{2}}=(\frac{D}{p})=(-1)^n$. Let $D=q\neq p$ then either $x=\rho_x+g_x \pmod 2$ or $x=\rho_x+g_x+1 \pmod 2$, depending on whether $\rho_x>0$ or $\rho_x<0$. Fix $D=q$. $\sum_{x=1}^{\frac{p-1}{2}}x=n+\sum_{x=1}^{\frac{p-1}{2}}\rho_x+\sum_{x=1}^{\frac{p-1}{2}}g_x \pmod 2$. Since $\sum_{x=1}^{\frac{p-1}{2}}x=\sum_{x=1}^{\frac{p-1}{2}}|\rho_x| \pmod p$, $\sum_{x=1}^{\frac{p-1}{2}}x=\sum_{x=1}^{\frac{p-1}{2}}\rho_x \pmod 2$. Thus, $n=\sum_{x=1}^{\frac{p-1}{2}}g_x \pmod 2$. Now $g_x=\lfloor\frac{qx}{p}\rfloor$, so $(\frac{q}{p})=(-1)^{\sum_{x=1}^{\frac{p-1}{2}}g_x}=(-1)^{\sum_{x=1}^{\frac{p-1}{2}}\lfloor\frac{qx}{p}\rfloor}$. Thus $(\frac{p}{q})(\frac{q}{p})=(-1)^{\sum_{x=1}^{\frac{p-1}{2}}\lfloor\frac{qx}{p}\rfloor+\sum_{y=1}^{\frac{q-1}{2}}\lfloor\frac{py}{q}\rfloor}$. Now use the fact that $\sum_{x=1}^{\frac{p-1}{2}}\lfloor\frac{xq}{p}\rfloor+\sum_{y=1}^{\frac{q-1}{2}}\lfloor\frac{yp}{q}\rfloor=\frac{(p-1)(q-1)}{4}$. This can be derived by looking at the number of lattice points not on the x or y axis in a $\frac{p}{2}\times\frac{q}{2}$ rectangle with diagonal verticies at $(0,0)$ and $(\frac{p}{2},\frac{q}{2})$. Let $S=\{(x,y):1\leq x\leq\frac{p-1}{2},1\leq y\leq\frac{q-1}{2}\}$, so $|S|=\frac{p-1}{2}\cdot\frac{q-1}{2}$. $S_1=\{(x,y)\in S:qx>py\}$ and $S_2=\{(x,y)\in S:qx<py\}$. $|S_1|=\sum_{x=1}^{\frac{p-1}{2}}\lfloor\frac{qx}{p}\rfloor$. Similarly, $|S_2|=\sum_{y=1}^{\frac{q-1}{2}}\lfloor\frac{py}{q}\rfloor$ and $S=S_1\cup S_2$.

Another Proof of QR using Gauss Sums: $g_a(\zeta)=\sum_{t=0}^{p-1}\zeta(t)\varsigma^{at}$. Set $g(x)=g_1(x)$. Number of solutions to $x^2=t \pmod p$ is $1+(\frac{t}{p})$. $g_a(\zeta)=\zeta(a^{-1})g(\zeta)$ if $a\neq 0 \pmod p$ otherwise it's 0. $\sum(\frac{t}{p})\varsigma^{at}=(\frac{a}{p})\sum(\frac{t}{p})\varsigma^t$. If ζ is the principal character, $g(\zeta)=\sqrt{p}$. If ζ is real and $g^k(\zeta)=(g(\zeta))^k$ then $g^2(\zeta)=(-1)^{\frac{p-1}{2}}p$. Look at $|g(\zeta)|^2=T=\sum_a g_a(\zeta)\overline{g}_a(\zeta)$. On one hand, it's $\sum_t(\frac{t}{p})(\frac{-t}{p})g^2=(\frac{-1}{p})(p-1)g^2$. On the other, it's $\sum_x\sum_y\sum_a g_a(\zeta(x))g_{-a}(\zeta(y))=\sum_a\sum_x\sum_y(\zeta(xy))\varsigma^{(x-y)a}=(p-1)p$.

Now set $p^* = (-1)^{\frac{p-1}{2}}p$. $g^{q-1} = (g^2)^{\frac{q-1}{2}} = (\frac{p^*}{q})$. So $g^q = (\frac{p^*}{q})g$. On the other hand, $g^q = (\sum_t (\frac{t}{p})\varsigma^t)^q \pmod q = (\sum_t (\frac{t}{p})^q \varsigma^{qt}) \pmod q = (\frac{q}{p})g$. So $(\frac{p^*}{q}) = (\frac{q}{p})$.

Theorem: $b^n + 1$ is prime only if n is a power of 2. If $M_p = 2^p - 1$ is prime, $\Delta_M = \frac{1}{2}M(M+1)$ is perfect.

Beatty: If $\frac{1}{\alpha} + \frac{1}{\beta} = 1$ and $A = \{\lfloor m\alpha \rfloor\}$, $B = \{\lfloor m\beta \rfloor\}$ then $A \cup B = Z$ and $A \cap B = \emptyset$.

Pell's Equation: $x^2 - dy^2 = 1$ is solvable (if d is not a perfect square) using continued fractions. Let $\frac{p}{q} < \frac{r}{s}$ be two rationals such that $ps - rq = -1$ then $\forall \lambda, \mu$, $\frac{p}{q} \leq \frac{\lambda p + \mu r}{\lambda q + \mu s} \leq \frac{r}{s}$. Let $\frac{p}{q} \leq \frac{a}{b} \leq \frac{r}{s}$ with $ps - rq = -1$ then $a = \lambda p + \mu r$ and $b = \lambda q + \mu s$.

Primes in arithmetic progressions: There are infinitely many primes of the form $4n + 3$. **Dirichlet:** If $a > 0$ and $(a, n) = 1$, then there are infinitely many primes p, such that $p = a \pmod n$. Largest power of p dividing $n!$ is $\sum_{l \geq 0} \lfloor \frac{n}{p^l} \rfloor$.

Bertrand's Postulate: For any n there is a prime p: $n < p < 2n$.

Outline of Erdos' proof:

(1) Prove for $n < 4000$.

(2) $\prod_{p \leq n} p \leq 4^n$.

This is true for $n \leq 4$. If $n > 3$ is even, $\prod_{p \leq n-1} p \leq \prod_{p \leq n} p \leq 4^{n-1}$ by induction. Suppose $n > 3$ is odd and put $k = \frac{n \pm 1}{2}$ choosing the odd outcome. $\prod_{k < p \leq n} p \leq \binom{n}{k}$. Since $\binom{n}{k} = \binom{n}{n-k}$ and both appear in the expansion of $(1+1)^n$, $\binom{n}{k} \leq 2^{n-1}$ and $\prod_{p \leq n} p = (\prod_{p \leq k} p)(\prod_{k < p \leq n} p) < 4^k \cdot 2^{n-1} = 4^n$.

(3) Let μ_p be the exponent of the largest power of p that divides $\binom{2n}{n}$ and $\nu_p : p^{\nu_p} \leq 2n < p^{1+\nu_p}$. Suppose the result is false for some $n \geq 4000$ then $\binom{2n}{n} = \prod_{p \leq 2n} p^{\mu_p} = \prod_{p \leq n} p^{\mu_p}$, $\mu_p \leq \nu_p$. If $\frac{2n}{3} < p \leq n$, we have $p \geq 3, p^2 > \frac{2}{3}np \geq 2n$ and $1 \leq \frac{n}{p} < \frac{3}{2}$ and $2 \leq \frac{2n}{p} < 3$ so $\mu_p = \lfloor \frac{2n}{p} \rfloor - 2\lfloor \frac{n}{p} \rfloor = 0$. If $\sqrt{2n} < p \leq \frac{2n}{3}$, we have $p^2 > 2n$ and $\nu_p = 1, \mu_p \leq 1$. For $p < \sqrt{2n}$, $p^{\mu_p} \leq p^{\nu_p} \leq 2n$ and all together we have $\binom{2n}{n} = (\prod_{p \leq \sqrt{2n}} p^{\mu_p})(\prod_{\sqrt{2n} < p \leq \frac{2n}{3}} p^{\mu_p})(\prod_{\frac{2n}{3} < p \leq 2n} p^{\mu_p}) \leq (\prod_{p \leq \sqrt{2n}} 2n)(\prod_{p \leq \frac{2n}{3}} p)$. So $\binom{2n}{n} \leq (2n)^{\sqrt{2n}-2} 4^{\frac{2n}{3}}$, $2^{\frac{2n}{3}} < (2n)^{\sqrt{2n}}$.

(4) Since $\binom{2n}{n}$ is the largest term in $(1+1)^{2n}$, $(2n+1)\binom{2n}{n} > 2^{2n}$ and since $4n^2 > 2n + 1$, $4n^2\binom{2n}{n} > 2^{2n}$ and $\binom{2n}{n} > 2^{2n}(2n)^{-2}$. Thus $2^{\frac{2n}{3}} < 2^{\sqrt{2n}}$ which can only happen if $n \leq 450$ and the theorem holds.

Theorem: The following moduli have *primitive roots* for $p > 2$, $2, 4, p^k, 2p^k$. Fact for **Miller-Rabin:** $n - 1 = 2^s r$, $r \neq 0 \pmod 2$, $(a, n) = 1$. If n is prime, either $a^r = 1 \pmod n$ or $a^{2^j r} = -1 \pmod n$ for some $j : 0 \leq j \leq (s-1)$.

Definitions: The *Reimann zeta function* is $\zeta(s) = \sum \frac{1}{n^s}$ which converges for $Re(s) > 1$. Note: $\zeta(2) = \frac{\pi^2}{6}$. *Riemann hypothesis:* If $s = a + bi$, all the zeros of $\zeta(s)$ have $a = \frac{1}{2}$.

Prime Number Theorem: Let $\Pi(x)$ be the number of primes $\leq x$. $\Pi(x) \approx (\frac{x}{ln(x)})$.

Proof of weaker result: $\exists a,b \in \mathbb{R} : a\frac{x}{ln(x)} < \pi(x) < b\frac{x}{ln(x)}, a = \frac{ln(2)}{4}, b = 9ln(2)$.

Let μ_p and ν_p be defined as in Bertrand's postulate. $\lfloor \frac{2n}{p^j} \rfloor - 2\lfloor \frac{n}{p^j} \rfloor = 0, j \geq \nu_p$ further, $\lfloor \frac{2n}{p^j} \rfloor - 2\lfloor \frac{n}{p^j} \rfloor \leq 1, j \geq 1$ so $\mu_p \leq \nu_p$ and $\binom{2n}{n} \mid \prod_{p \leq 2n} p^{\nu_p}$. If $n < p \leq 2n$, $p \mid (2n)!$ but $p \nmid n!$ so $\prod_{n<p\leq 2n} p \leq \binom{2n}{n} \leq \prod_{n<p\leq 2n} p^{\nu_p} \leq \prod_{p\leq 2n} 2n$. So $n^{\pi(2n)-\pi(n)} \leq \binom{2n}{n} \leq (2n)^{\pi(2n)}$. Taking logs, $\pi(2n) - \pi(n) \leq \frac{2nln(2)}{ln(2n)}$ and $\pi(2n) \geq \frac{nln(2)}{ln(n)}, n > 1$. Let $2n$ be the greatest even integer in x then the second inequality gives $\pi(x) \geq \pi(2n) \geq \frac{nln(2)}{ln(2n)} \geq \frac{nln(2)}{ln(x)} \geq \frac{(2n+2)ln(2)}{4ln(x)} > \frac{ln(2)}{4}\frac{x}{ln(x)}$. For the reverse inequality, $y \geq 4$, let $2n$ be the smallest even integer $\geq y$ so $y \leq 2n, \pi(y) \leq \pi(2n), y+2 > 2n, \frac{y}{2} > n-1$. Thus $\pi(\frac{y}{2}) \geq \pi(n-1) \geq \pi(n)-1$ and $\pi(y) - \pi(\frac{y}{2}) \leq \pi(2n) - \pi(n) + 1 \leq \frac{2nln(2)}{ln(y)} + 1 \leq \frac{2(y+2)ln(2)}{ln(y)} + 1 \leq \frac{3yln(2)}{ln(y)} + 1 \leq \frac{4yln(2)}{ln(y)}$. So $\pi(y) - \pi(\frac{y}{2}) \leq \frac{4yln(2)}{ln(y)}$ for $y \geq 2$. For $2 \leq y < 4$, $\pi(y) - \pi(\frac{y}{2}) \leq \pi(4)$ and so $\pi(y) - \pi(\frac{y}{2}) \leq \frac{2/e)y}{ln(y)}, y \geq 2$. Hence, $\pi(y)ln(y) - \pi(\frac{y}{2})ln(\frac{y}{2}) = \pi(y) - \pi(\frac{y}{2})ln(y) + \pi(\frac{y}{2})ln(2) < 4yln(2) + \frac{y}{2}ln(2) = \frac{9}{2}yln(2)$ and this proves the upper bound.

Euler's Formula: $\sum_{y<n\leq x} f(n) = \int_y^x f(t)dt + \int_y^x (t - \lfloor t \rfloor)f'(t)dt + (x - \lfloor x \rfloor)f(x) - (y - \lfloor y \rfloor)f(y)$.

Theorem: $\sum_{n\leq x} \frac{1}{n} = ln(x) + C + O(\frac{1}{x})$. $\sum_n \frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}$.

Dirichlet: Let α be a real number and Q a positive integer. There is a rational number $\frac{p}{q}$ with $1 \leq q \leq Q$ such that $|\alpha - \frac{p}{q}| \leq \frac{1}{qQ}$.

Proof: Let $B_q = \{\frac{q-1}{Q} \leq x < \frac{q}{Q}\}$. Let $c_q = q\alpha - \lfloor q\alpha \rfloor$. By the pigeon hole principle, at least 2 c_q's must lie in a single B_k. This completes the proof. It's easy to extend this to show that if α is irrational, there are infinitely many rational numbers $\frac{p}{q}$ such that $|\alpha - \frac{p}{q}| \leq \frac{1}{q^2}$, which was sharpened by Hurwitz.

Hurwitz: If α is irrational, there are infinitely many rational numbers $\frac{p}{q}$ such that $|\alpha - \frac{p}{q}| \leq \frac{1}{\sqrt{5}q^2}$.

Liouville: Let α be an algebraic number of degree $d \geq 2$. There is a constant $c(\alpha) > 0$ such that for all $\frac{p}{q}$, $|\alpha - \frac{p}{q}| > \frac{c(\alpha)}{q^d}$ has only finitely many solutions.

Proof: Suppose $f(\xi) = a_n\xi^n + a_{n-1}\xi^{n-1} + \ldots + a_0$. $\exists M : |f'(y)| < M, \forall y : \xi - 1 < y < \xi + 1$. If $\xi - 1 < \frac{p}{q} < \xi + 1$ and $f(\frac{p}{q}) \neq 0$ so $|f(\frac{p}{q})| = \frac{|a_n p^n + a_{n-1}p^{n-1}q + \ldots + a_0 q^n|}{q^n} \geq \frac{1}{q^n}$. $f(\frac{p}{q}) = f(\frac{p}{q}) - f(\xi) = (\frac{p}{q} - \xi)f'(\eta)$. Therefore, $|\frac{p}{q} - \xi| = \frac{|f(\frac{p}{q})|}{|f'(\eta)|} > \frac{1}{Mq^n}$, proving the theorem.

Roth: Let α be an algebraic number of degree $d \geq 2$ and $\epsilon > 0$. There is a constant $c(\alpha, \epsilon) > 0$ such that for all $\frac{p}{q}$, $|\alpha - \frac{p}{q}| > \frac{c(\alpha,\epsilon)}{q^{2+\epsilon}}$. Consequence: $z = \sum_i^\infty 10^{-i!}$ is transcendental.

Theorem: $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$.

Proof: Let $a = bq + r$, $x^a - 1 = (x^b - 1)(x^{a-b} + x^{a-2b} + \ldots + x^{a-qb}) + x^r - 1$. This parallels the construction of (a, b) in the Euclidean algorithm.

Definition: If $x = p^k\frac{a}{b}, (a, b) = (a, p) = (b, p) = 1$ then $\nu_p(x) = k$ is a *p-adic valuation.* If $f(x, y, z)$ over $\mathbb{Z}$ is quadratic, then f has a solution over $\mathbb{Z}$ iff it has a solution in the p-adics over for all p. *Counterexample for higher order equations:* $3x^3 + 4y^3 + 5z^3 = 0 \pmod p$ is solvable for p but $3x^3 + 4y^3 + 5z^3 = 0$ has no solutions.

Lemma: 2 is a QR $\pmod p$ if $p = 1, 7 \pmod 8$, 2 is not a QR $\pmod p$ if $p = 3, 5 \pmod 8$. $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$.

Proof: Second part follows from first.

Lemma: Suppose $\zeta = \zeta_n = e^{\frac{2\pi i}{n}}$. If n is odd, $x^n - y^n = \prod_{k=0}^{n-1}(\zeta^k x - \zeta^{-k} y)$.

Proof: $x^n - y^n = \prod_{k=0}^{n-1}(x - \zeta^{-2k} y) = \zeta^{1+2+\ldots+n-1} \prod_{k=0}^{n-1}(x\zeta^k - \zeta^{-k} y)$. Since $n|(1+2+\ldots+n-1)$, the result follows.

Lemma: If n is odd and $f(x) = e^{2\pi i} - e^{-2\pi i}$, $\frac{f(nz)}{f(z)} = \prod_{k=1}^{\frac{n-1}{2}} f(z + \frac{l}{n}) f(z - \frac{l}{n})$.

Proof: Put $f(z) = e^{2\pi iz} - e^{-2\pi iz}$. Let $x = e^{2\pi iz}$ and $y = e^{-2\pi iz}$ in the Lemma above. $\frac{f(nz)}{f(z)} = \prod_{k=1}^{n-1} f(z + \frac{k}{n}) = \prod_{k=1}^{\frac{n-1}{2}} f(z + \frac{k}{n}) f(z - \frac{k}{n})$.

Lemma: If p is odd prime, $a \in \mathbb{Z}$ and $p \nmid a$ then $\prod_{l=1}^{\frac{p-1}{2}} f(\frac{la}{p}) = (\frac{a}{p}) \prod_{l=1}^{\frac{p-1}{2}} f(\frac{l}{p})$.

Proof: If $1 \le l < p$, $la = \pm m_l \pmod p$, so $f(\frac{la}{p}) = f(\frac{\pm m_l}{p})$. Take the product over all l from 1 to $\frac{p-1}{2}$ and apply Gauss' lemma ($(\frac{a}{p}) = (-1)^\mu$ where μ is the number of negative least residues.

Yet another proof of QR:

Proof: So $(\frac{q}{p}) = \frac{\prod_{l=1}^{\frac{p-1}{2}} f(\frac{lq}{p})}{\prod_{l=1}^{\frac{p-1}{2}} f(\frac{l}{p})} = \prod_{m=1}^{\frac{q-1}{2}} \prod_{l=1}^{\frac{p-1}{2}} f(\frac{l}{p} + \frac{m}{q}) f(\frac{l}{p} - \frac{m}{q})$ and $(\frac{p}{q}) = \prod_{m=1}^{\frac{q-1}{2}} \prod_{l=1}^{\frac{p-1}{2}} f(\frac{m}{q} + \frac{l}{p}) f(\frac{m}{q} - \frac{l}{p})$. Since $f(-t) = -f(t)$, $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. $\prod_{l=1}^{\frac{p-1}{2}} f(\frac{lq}{p}) = (\frac{q}{p} \prod_{l=1}^{\frac{p-1}{2}} f(\frac{l}{p})$.

Lemma: $\sum_{t=0}^{p-1} \zeta_p^{at} = p$, if $a = 0 \pmod p$ and 0 otherwise.

Proof: $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \ldots + 1)$. Substituting $x = \zeta_p^{at}$ gives the result.

Definition: $Z_f(u) = exp(\sum_{s=1}^{\infty} \frac{N_s}{s} u^s)$ where N_s is the number of solutions of $f(u) = 0$ in $\mathbb{P}^n(F_{q^s})$.

1.1.2 Inequalities

Arithmetic-Geometric: $\frac{1}{n}\sum_n a_i \ge (\prod_n a_i)^{\frac{1}{n}}$.

Proof:

Lemma 1: $\frac{a+b}{2} \ge \sqrt{ab}$.
Proof of Lemma 1: $(\sqrt{a} - \sqrt{b})^2 \ge 0$. So $a + b - 2\sqrt{ab} \ge 0$ and the result follows.

Lemma 2: If $n = 2^k$ then $\frac{\sum_{i=1}^n a_i}{n} \ge (\prod_{i=1}^n a_i)^{\frac{1}{n}}$.
Proof of Lemma 2: Proof by induction on k. True for $k = 1$, trivially and true for $k = 2$ by Lemma 1. Suppose $n = 2^{k+1}$ and the lemma is true for $n = 2^k$. $\frac{\sum_{i=1}^n a_i}{n} = \frac{1}{2}[\frac{\sum_{i=1}^{n/2} a_i}{n/2} + \frac{\sum_{i=n/2+1}^n a_i}{n/2}] \ge \frac{1}{2}[(\prod_{i=1}^{n/2} a_i)^{2/n} + (\prod_{i=n/2+1}^n a_i)^{2/n}]$ by the induction hypothesis. Now $\frac{1}{2}[(\prod_{i=1}^{n/2} a_i)^{2/n} + (\prod_{i=n/2+1}^n a_i)^{2/n}] \ge \sqrt{(\prod_{i=1}^{n/2} a_i)^{2/n}} \sqrt{(\prod_{i=n/2+1}^n a_i)^{2/n}}$ by Lemma 1 and $\sqrt{(\prod_{i=1}^{n/2} a_i)^{2/n}} \sqrt{(\prod_{i=n/2+1}^n a_i)^{2/n}} = (\prod_{i=1}^n a_i)^{1/n}$ concluding the proof of Lemma 2.

For the case when n is not a power of 2, let $2^k < n < 2^{k+1} = m$ and let $\alpha = \frac{\sum_{i=1}^n a_i}{n}$. $\alpha = \frac{\sum_{i=1}^n a_i}{n} = \frac{\sum_{i=1}^n (\frac{m}{n} a_i)}{m} = (\frac{1}{m})(\frac{\sum_{i=1}^n a_i}{n} + \sum_{i=n+1}^m \alpha) \ge ((\prod_{i=1}^n a_i)(\prod_{i=n+1}^m \alpha))^{\frac{1}{m}}$ where the last inequality follows from Lemma 2. Thus we have $\alpha = \frac{\sum_{i=1}^n a_i}{n} \ge ((\prod_{i=1}^n a_i)(\prod_{i=n+1}^m \alpha))^{\frac{1}{m}} = ((\prod_{i=1}^n a_i)\alpha^{m-n})^{\frac{1}{m}}$. Raising both sides to the m-th power and dividing by α^{m-n}, we get $\alpha^n \ge (\prod_{i=1}^n a_i)$ and the theorem follows.

Triangle Inequality: $|x| + |y| \geq |x + y|$.

Cauchy-Schwartz: $|u \cdot v| \leq ||u||||v||$.

Proof: Look at $\sum (a_i x + b_i)^2$. Get $(\sum {a_i}^2)x^2 + 2(\sum a_i b_i)x + \sum {b_i}^2$. Complete square. Constant is always ≥ 0.

Holder's inequality: If $\frac{1}{p} + \frac{1}{q} = 1$ then $\frac{{a^p}}{p} + \frac{{b^q}}{q} \geq ab$ and $(\sum_i {a_i}^p)^{\frac{1}{p}} \cdot (\sum_i {b_i}^q)^{\frac{1}{q}} \geq \sum_i a_i b_i$.

Proof: If f is monotonically increasing, $f(0) = 0$, then $\int_0^a f + \int_0^b f^{-1} \geq ab$.

Another proof: You can prove first part using Arithmetic-Geometric inequality. Apply this inequality repeatedly with $a = \frac{a_i}{(\sum_{i=1}^n {a_i}^p)^{\frac{1}{p}}}$ and $b = \frac{b_i}{(\sum_{i=1}^n {b_i}^q)^{\frac{1}{q}}}$. Adding these we get $(\sum_{i=1}^n {a_i}^p)^{\frac{1}{p}} (\sum_{i=1}^n {b_i}^q)^{\frac{1}{q}} \geq \sum_{i=1}^n a_i b_i$.

Minkowski's inequality: $(\sum {a_i}^p)^{\frac{1}{p}} + (\sum {b_i}^p)^{\frac{1}{p}} \geq (\sum (a_i + b_i)^p)^{\frac{1}{p}}$.

Proof: Write $(x_1 + x_2)^p + (y_1 + y_2)^p = [(x_1 + x_2)^{p-1} x_1 + (y_1 + y_2)^{p-1} y_1] + [(x_1 + x_2)^{p-1} x_2 + (y_1 + y_2)^{p-1} y_2]$. Apply Holder to each term to get $(x_1^p + y_1^p)^{\frac{1}{p}} [(x_1 + x_2)^{(p-1)q} + (y_1 + y_2)^{(p-1)q}]^{\frac{1}{q}} \geq x_1 (x_1 + x_2)^{p-1} + y_1 (y_1 + y_2)^{p-1}$ and $(x_2^p + y_2^p)^{\frac{1}{p}} [(x_1 + x_2)^{(p-1)q} + (y_1 + y_2)^{(p-1)q}]^{\frac{1}{q}} \geq x_2 (x_1 + x_2)^{p-1} + y_2 (y_1 + y_2)^{p-1}$. Since $\frac{1}{p} + \frac{1}{q} = 1$, $(p-1)q = p$. Adding the two inequalities and dividing by $[(x_1^p + x_2^p) + (y_1^p + y_2^p)]^{\frac{1}{q}}$ while noting that $1 - \frac{1}{q} = \frac{1}{p}$, we get Minkowski.

Chebyshev's inequality: If $a_1 \leq a_2 \ldots \leq a_n$, $b_1 \leq b_2 \ldots \leq b_n$ $(\frac{1}{n} \sum a_i)(\frac{1}{n} \sum b_i) \leq (\frac{1}{n} \sum a_i b_i)$.

Proof: By the rearrangement inequality, $a_1 b_1 + a_2 b_2 + \ldots + a_n b_n \geq a_1 b_1 + a_2 b_2 + \ldots + a_n b_n$, $a_1 b_1 + a_2 b_2 + \ldots + a_n b_n \geq a_1 b_2 + a_2 b_3 + \ldots + a_n b_1$, ... $a_1 b_1 + a_2 b_2 + \ldots + a_n b_n \geq a_1 b_n + a_2 b_1 + \ldots + a_n b_{n-1}$. Adding the n inequalities, we get $n \sum a_i b_i \geq a_1 \sum b_j + a_2 \sum b_j + \ldots + a_n \sum b_j$ or $n \sum a_i b_i \geq (\sum a_i)(\sum b_j)$.

Observation: $\sum_i a_i b_i$ is max when a_i and b_i are in order, $a_i b_i \geq 0$. $min(a, b) \leq \frac{2ab}{a+b} \leq \sqrt{a}b \leq \frac{a+b}{2} \leq \sqrt{\frac{a^2+b^2}{2}} \leq max(a, b)$.

Definitions: *Concave (convex downwards, convex cap — like $-x^2$): $f(tx + (1-t)y) \geq tf(x) + (1-t)f(y)$. Convex (convex upwards, convex cup— like x^2): $f(tx + (1-t)y) \leq tf(x) + (1-t)f(y)$.*

Jensen's Theorem: If f is convex, $E(f(X)) \leq f(E(X))$. If f is concave, $E(f(X)) \geq f(E(X))$. Consequence: $log(x) \leq (x - 1)$, equality iff $x = 1$.

Proof: Let $\lambda_1 + \lambda_2 = 1$ then $f(\lambda_1 x + \lambda_2 y) \leq \lambda_1 f(x) + \lambda_2 f(y)$, by definition. Now apply induction.

Hadamard inequality: $|D(a_1, a_2, a_3, \ldots, a_n)| \leq ||a_1|| \cdot ||a_2|| \ldots \cdot ||a_n||$. $a^2 + b^2 + c^2 \geq ab + ac + bc$ and $\frac{b}{a+c} + \frac{a}{b+c} + \frac{c}{b+c} \geq \frac{3}{2}$.

Weighted AM-GM: If $\lambda_1, \ldots, \lambda_n > 0$ and $\sum_{i=1}^n \lambda_i = 1$, then $\sum_{i=1}^n \lambda_i x_i \geq \prod_{i=1}^n x_i^{\lambda_i}$.

1.1.3 Combinatorics and Sets

Let $f(x) = c_k x^k + \ldots + c_0$ be a polynomial with $c_0 c_k \neq 0$ which factors as $f(x) = c_k(x - r_1)^{m_1} \ldots (x - r_l)^{m_l}$, then a sequence $\{a_n\}$ satisfies a *linear recurrence* with characteristic polynomial $f(x)$ iff $\exists : g_1(x), \ldots, g_l(x)$ such that $a_n = g_1(n){r_1}^n + \ldots + g_l(n){r_l}^n$ where $deg(g_i) < m_i$.

> *Proof:* Put $a_n = a_j {\alpha_j}^n$ where $f(\alpha_j) = 0$. Then $c_k {\alpha_j}^k + \ldots + c_0 = 0$. These solutions are linearly independent for $1 \leq j \leq k$, so the general solution is a linear combination of these solutions.

Power Means: If $k_1 \geq k_2$ and $a_i \geq 0$ then $(\sum_{i=1}^n \frac{a_i^{k_1}}{n})^{k_2} \geq (\sum_{i=1}^n \frac{a_i^{k_2}}{n})^{k_1}$.

> *Proof:* $(\sum_{i=1}^n \frac{a_i^{k_1}}{n})^{\frac{1}{k_1}} \leq (\sum_{i=1}^n \frac{a_i^{k_2}}{n})^{\frac{1}{k_2}}$, so $(\sum_{i=1}^n \frac{a_i^{k_1}}{n}) \leq (\sum_{i=1}^n \frac{a_i^{k_2}}{n})^{\frac{k_1}{k_2}}$. $f(x) = x^{\frac{k_2}{k_1}}$ is concave, so applying Jensen: $(\sum_{i=1}^n \frac{a_i^{k_1}}{n})^{\frac{k_2}{k_1}} \geq (\sum_{i=1}^n \frac{a_i^{k_2}}{n})$. So

Linear congruential generator: $x_{n+1} = (ax_n + c) \pmod m$ has period n if $(c, m) = 1$. $b = a - 1$, $b = 0(p)$ if $p|m, b = 0(4)$ if $m = 0(4)$.

Burnside counting: Let a permutation group G act on A inducing an equivalence relation S. Let n be the number of equivalence classes. $n = \frac{1}{|G|} \sum_{g \in G} |A_g|$.

> *Proof:* Count $S = \{(a, g), a \in A, g \in G : a^g = a\}$ two different ways.

Notation: Let D be a set of elements permuted by a group G and R be a set of colors. A *coloring* is a map $f : D \to R$. The set of colorings is denoted by R^D. Two colorings, f_1, f_2, are *equivalent* if $f_1(d) = f_2(d^g), \forall d$. Let w be a map from R to a set of *weights*. The term $\sum_{r \in R} w(r)$ is called the *store*. If $f : D \to R$ then $W(f) = \prod_{d \in D} w(f(d))$ is called the weight of f. If F is a set of functions from $D \to R$, $\mathcal{I}(F) = \sum_{f \in F} W(f)$. If F_G consists of a representative of each equivalence class under G of F, $\mathcal{I}(F_G)$ is called the *pattern inventory*. Suppose $F = \bigcup_i F_i$ where F_i are a set of functions of weight i and suppose $\pi \mapsto \pi^{(i)}$ is the homomorphisms that take permutations of D to the action induced by equivalent coloring on the functions of F_i. Let $cyc(\pi)$ be the number of cycles in π. Finally, define $P_G(x_1, x_2, \ldots, x_n) = \frac{1}{|G|} \sum_{g \in G} x_1^{\pi_1(g)} x_2^{\pi_2(g)} \ldots x_n^{\pi_n(g)}$, where π_i is the number of cycles of length i in g. *Example:* Consider a string of three beads colored either r or b. $D = \{1, 2, 3\}$ and $R = \{r, b\}$. $G = \langle(13)\rangle$ so that the order of beads on a string doesn't matter. $P_G(x_1, x_2) = \frac{1}{2}(x_1^3 + x_1 x_2)$. Let F be a set of representatives of colorings from each equivalence class. $\mathcal{I}(F_G) = \frac{1}{2}[(r + b)^3 + (r + b)(r^2 + b^2)] = b^3 + 2r^2 b + 2b^2 r + r^3$, so there are six distinct (under the action of G) patterns.

Observation: Let $D_1, D_2, \ldots, D_k$ be a partition of D into disjoint sets. Since $\sum_{r \in R} w(r)^{|D_i|}$ is a representation of the number of ways to distribute the objects in D_i so they will end up in the same color, $\prod_{i=1}^k [\sum_{r \in R} w(r)^{|D_i|}]$ is the inventory of D^R in which elements of each D_i have the same color.

Polya's Theorem: Let F be a set of functions from $D \to R$, $\mathcal{I}(F_G) = P_G(\sum_r w(r), \sum_r w(r)^2, \ldots, \sum_r w(r)^k, \ldots)$.

> *Proof:* Let $F = \bigcup_i F_i$ and m_i be the number of equivalence classes of weight W_i in F_i then, by Burnside, $\mathcal{I}(F_G) = \sum_i m_i W_i = \sum_i \frac{1}{|G|} \sum_{g \in G} \psi(g^{(i)}) W_i = \frac{1}{|G|} \sum_{g \in G} (\sum_i \psi(g^{(i)})) W_i$ where $\psi(g^{(i)})$ is the number of colorings fixed by $g^{(i)}$. Note that $(\sum_i \psi(g^{(i)})) W_i$ is the inventory of all equivalent f and so $\sum_i \psi(g^{(i)}) W_i = \prod_j (\sum_r w(r)^j)^{b_j}$ where b_j is the number of cycles of length j in g. This completes the proof.

Example (Vertices on cube): $P_G = \frac{1}{24}(x_1^8 + 9x_2^4 + 6x_4^2 + 8x_1^2 x_3^2)$. For two colors, the number of patterns is 23.
Example (Faces on cube): $P_G = \frac{1}{24}(x_1^6 + 6x_1^2 x_4 + 3x_1^2 x_2^2 + 6x_2^3 + 8x_3^2)$. For $f \in R^D$, store: $\sum w(r)$, inventory:

$W(f) = \prod_d f(d)$, pattern inventory of $R^D = \sum_f W(f)$.

Corollary: Number of equivalence classes= $P_G(|R|, |R|, \ldots |R|)$.

Proof: Assign a weight of 1 to each element of R and apply Polya.

$(\mathbf{v}, \mathbf{k}, \mathbf{t}, \lambda)$ **design:** $|X| = v$, B is a set of k subsets of X is a design if each t subset T of X, the number of blocks containing T is λ and $|B| = b$. r, the incidence number, is the number of blocks incident with one point. These designs are denoted $t-(v,k,\lambda)$ or $S_\lambda(t,k,v)$. $b_i = \lambda \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}}$, $b_0 = b$, $b_1 = r$. $\frac{(vr)}{k} \leq \binom{v}{k}$.

Hall's Theorem: $J(A) = \{y \in Y, (x,y) \in E, x \in A\}$ and $|J(A)| \geq |A|$ if and only if there is a complete matching.

Inclusion-Exclusion: Let $A_1, A_2, \ldots, A_n$ be a family of subsets of X. The elements of X that are not in $\bigcup_i^n A_i$ is $\sum_{I \subseteq [n]} (-1)^{|I|} |A_I|$ where $A_I = \bigcap_{i \in I} A_i$. (Note: $A_\phi = X$.) For classical statement, let $A_i = \{x : c_i(x) \; is \; true\}$. Somtimes this is written $N(\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}) = N - \sum_i N(a_i) + \sum_{i,j} N(a_i, a_j) + \sum_{i,j,k} N(a_i, a_j, a_k) - \ldots + (-1)^n N(a_1, a_2, \ldots, a_n)$.

Ramsay: Let $P_r(S)$ be the r-subsets of S. Let $P_r(S) = A_1 \cup \ldots \cup A_t$ and $1 \leq r \leq q_1, \ldots q_t$. $\exists N(r, q_1, \ldots q_t)$ such that for $n \geq N$, S contains a (q_i, A_i). $R(m,n) \leq R(m-1,n) + R(m,n-1)$ and $R(s,t) \leq \binom{(s+t-2)}{(s-1)}$.

Generating Functions: Let 12 objects be distributed to A, B, C subject to: A gets at least 4, B and C get at least 2 and C gets no more that 5. The coefficient of x^{12} in $(x^4 + \ldots x^8)(x^2 + \ldots x^8)(x^2 + \ldots x^5)$ is the number of ways this can happen. For selections with repetitions note that: $(\frac{1}{1-x})^n = \sum_i \binom{n+i-1}{i} x^i$. For partitions, examine $\frac{1}{1-x}(\frac{1}{1-x})^2 \ldots$. Exponential generating functions: $f(x) = a_0 + a_1 x + \frac{1}{2!} a_2 x^2 + \ldots \frac{1}{k!} a_k x^k + \ldots$. Difference calculus: $\sum_i i^n = (1+\Delta)^n u_0$.

Counting results: *Dearrangements:* $n!(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} \ldots + (-1)^n \frac{1}{n!})$. *Menages (i is not in $i+1 \pmod n$):* $\sum_{r=0}^n (-1)^r (n-r)! \binom{(2n-r)}{r} \frac{2n}{2n-r}$. Number of solutions of $n_1 + n_2 + \ldots + n_r = r$ is $\binom{(n+r-1)}{r}$. *Restricted permutation positions:* $N(a_1', a_2', \ldots, a_{n-1}') = n! - \binom{n-1}{2}(n-2)! + \binom{n-1}{3}(n-3)! - \ldots + (-1)^n \binom{n-1}{n-1}(n-1)!$. For permutations of a, b, c, d, e, f which don't contain ace or fd: $N(a_1', a_2') = 6! - 4! - 5! + 3!$. *Rook polynomials:* $R(x,C) = xR(x,C_i) + R(x,C_e)$. *Forbidden positions:* $N(a_i', a_2', \ldots, a_n') = e_0 = n! - r_1(n-1)! + r_2(n-2)! - \ldots = \sum (-1)^j r_j (n-j)!$. *Exactly m with property:* $e_m = \sum_{j=0}^n (-1)^j \binom{m+j}{j} s_{m+j}$. *Fixed points in a random permutation:* Let $h : GF(2)^n \to GF(2)^n$ be a random permutation. The limit as $n \to \infty$ that h has p fixed points is $\frac{1}{pe}$.

Theorem: If the number of surjective maps from $[m] \to [n]$ is denoted $S(m,n)$, $S(m,n) = \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} k^m$. $n! = \sum_{i=0}^n (-1)^i \binom{n}{i} (n-i)^n$.

Proof: By induction on n. If $n > m$, $S(m,n) = 0$ and $S(m,0) = 4$ always. If $m \geq n \geq 1$, there are $\binom{n}{k}$ distinct k-subsets of $[n]$; any map is surjective on some k-subset so $n^m = \sum_{k=0}^n \binom{n}{k} S(m,k)$.
Now use the following
Lemma: If $B_n = \sum_{k=0}^n \binom{n}{k} A_k$ then $A_k = \sum_{k=0}^n \binom{n}{k} (-1)^{n+k} B_k$.

Proof of Lemma: $\sum_{k=0}^n \binom{n}{k} (-1)^{n+k} B_k = \sum_{k=0}^n \binom{n}{k} (-1)^{n+k} (\sum_{r=0}^k \binom{k}{r} A_r) = \sum_{k=0}^n \sum_{r=0}^k \binom{n}{k}\binom{k}{r} A_r)(-1)^{n+k}$. The coefficient of A_n in this sum is 1 and the coefficient of $A_r, r < n$, denoted λ_r in this sum is 0. $\lambda_r = \sum_{k=r}^n \binom{n}{k}\binom{k}{r}(-1)^{n+k}$ and the second term in the sum is equal to $\binom{(n-r)}{(k-r)}$, so $\lambda_r = (-1)^{n+k}\binom{n}{r} \sum_{j=0}^{n-r} \binom{(n-r)}{j}(-1)^{r+j} = 0$.

Multinomial coefficients: $\binom{a+b+c}{a,b,c}$ and $(x+y+z)^{a+b+c}$. $\binom{ne}{k} \leq (\frac{ne}{k})^k$, $\binom{n}{k} \geq (\frac{n}{k})^k$. Identities: $\binom{r}{k} = \frac{r}{k}\binom{r-1}{k-1}, \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \binom{r}{k} = (-1)^k\binom{k-r-1}{k}, \binom{r}{m}\binom{m}{k} = \binom{r}{k}\binom{r-k}{m-k}, \sum_{k=0}^{n}\binom{r+k}{k} = \binom{r+n+1}{n}, \sum_{k=0}^{n}\binom{k}{m} = \binom{n+1}{m+1}, \sum_{k=0}^{n}\binom{r}{k}\binom{s}{n-k} = \binom{r+s}{n}, \sum_{k=a}^{b-1} f(k) = \int_{k=a}^{b-1} f(x)dx + \sum_{k=1}^{m}\frac{B_k}{m!}f^{(k-1)}(x)_a^b + R_m, a_nT_n = b_nT_{n-1} + c_n \rightarrow s_na_nT_n = s_nb_nT_{n-1} + s_nc_n, s_nb_n = s_{n-1}a_{n-1}, R_n = s_na_nT_n, R_n = R_{n-1} + s_nc_n, \binom{-n}{r} = (-1)^r\binom{n+r-1}{r}, (1+x)^{-n} = 1 + \binom{-n}{1}x^{-1} + \ldots + \binom{-n}{n}x^{-n}$.

Definition: $S(n,k)$, or *Stirling numbers of the first kind*, is the number permutations in S_n with exactly k-cycles. $T(n,k)$, or *Stirling numbers of the second kind*, is the number of ways of grouping n objects into k groups. The *Bell numbers*, B_n, are the number of ways to divide n things into groups. $B_{n+1} = \sum_{k=0}^{n}\binom{n}{k}B_n$. $\sum_{k=0}^{n} S(n,k) = b_n, S(n+1,k) = kS(n,k) + S(n,k-1)$ $\sum_{k=0}^{n} T(n,k) = n!, T(n+1,k) = nT(n,k) + T(n,k-1)$. Let B_n denote the n-th *Bernoulli number* then $\sum_{j=0}^{m}\binom{m+1}{j}B_j = 0$ and $B_0 = 1$. $\frac{x}{e^x-1} = \sum_{n=0}^{\infty} B_n\frac{x^n}{n!}$. *Catalan numbers:* $c_n = \frac{1}{n+1}\binom{2n}{n}, c_n = \sum_{k=0}^{n-1} c_kc_{n-k-1}$.

Partitions: Let $p(n)$ be the number of partitions of n. Then, $p(n) \approx \frac{1}{4n\sqrt{3}}e^{\sqrt{\frac{2n}{3}}}$. The number of partitions of n into k things is the number of partitions of n with largest partition k.

A Theorem of Erdos: A sequence of $(n-1)(m-1)+1$ different numbers has either an increasing sub-sequence of length n or a decreasing sub-sequence of length m.

> *Proof:* Let $x \in B_r$ if the longest increasing sequence beginning with x has length n. If any B_r, with $r \geq n$ is non empty, we're done. Otherwise, there must be a B_k with $k < n$ containing at least m elements. These m elements form a decreasing sequence.
>
> Similarly, if $1 \leq a_1, \ldots, a_n \leq m$ and $1 \leq b_1, \ldots, b_n \leq m$, $\exists p, q, r, s$ with $a_{p+1} + \ldots + a_{p+q} = b_{r+1} + \ldots + b_{r+s}$. *Proof:* Let $j = j(k)$ be the smallest integer with $a_1 + \ldots + a_j \geq b_1 + \ldots + b_k$. Let $c_k = \sum_{i=1}^{j(k)} a_i - \sum_{i=1}^{k} b_i$. At least two c_l's (say c_u and c_v, $u > v$) are equal. $c_u - c_v$ provides the right sequence.

In permutation, $i < j$ and $a_i > a_j$ is *inversion*. Inversion table is (b_j) where b_j = number of elements left of j that are $> j$. For 5 9 1 8 2 6 4 7 3, it's 2 3 6 4 0 2 2 1 0. Inversion table uniquely determines permutation. Inverse has same number of inversions.

Generating permutations of $[1,n]$**:**

Set $\pi = 123\ldots n$. Output π.
If $\pi_i > \pi_{i+1}$, $\forall i$, stop.
Get largest i: $\pi_i < \pi_{i+1}$.
Find smallest j: $i < j$ such that $\pi_i < \pi_j$.
$\pi_i \leftrightarrow \pi_j$.
Reverse the order of the numbers following, π_j, denote this by π.
Output π. Go to 2.

Another algorithm: Steinhaus weaving generator (by recursion).

Definition: The *permanent*, $per(a_{ij})$, $m \times n$ matrix, is $\sum_\sigma a_{1i_1}a_{2i_2}\ldots a_{mi_m}$ where σ runs through m permutations of $[n]$. $n! = per(J) = \sum_{r=0}^{n-1}\binom{n}{r}(-1)^r(n-r)^n$. Let A_r be the matrix obtained by replacing r specified columns of A by 0. Let $S(A_r)$ be the product of row sums of A_r. Let $\sum_r S(A_r)$ over all choices of r: $per(A) = \sum S(A_{n-m}) - \binom{n-m+1}{1}S(A_{n-m+1}) + \ldots (-1)^{m-1}\binom{n-1}{m-1}S(A_{m-1})$.

Graph theory definitions: $\mathcal{G}(V, E)$ a graph with vertex set V and edge set E. $g(\mathcal{G})$ - girth - length of minimum cycle. $\omega(\mathcal{G})$- clique number. $\alpha(\mathcal{G}) = \omega(\overline{\mathcal{G}})$- independence number. $\chi(\mathcal{G})$ - chromatic number. $\delta(\mathcal{G})$ - minimum degree. $\Delta(\mathcal{G})$ - maximum degree. $d(x, y)$ = number of edges between x and y. $D_{\mathcal{G}}(x, y) = max_{x,y} d(x, y)$. Cayley graph. Strongly regular graphs. Expander graphs and short paths.

Theorem: A graph is *bipartite* iff it contains no cycles of odd length. $\alpha(\mathcal{G})\chi(\mathcal{G}) \geq n$.

Theorem: There are n^{n-2} labeled trees with n nodes.

> *Proof:* Use *Prufer code* for tree T: remove leaf with smallest label, add the label of the vertex it's connected to at end of sequence.

Graph counting: $G(n, M), N = \binom{n}{2}$. Random graph selecting M of the N edges. $Pr[G = H] = p^{e(H)}q^{N-e(H)}$. $X_s(G)$ = number of complete graphs of order s. $E(X_s) = \sum_{\alpha \in S} E(Y_\alpha(G)$, where $Y_\alpha(G) = 1$, if $G[\alpha] = K_\alpha$, 0 otherwise. $E_M(Y_\alpha) = P_M(G_p[\alpha] = K_\alpha) = p^S = \binom{N-S}{M-S}\binom{N}{M}^{-1}$. $E_p(X_s) = \binom{n}{s}p^s$. If a is the order of the automorphism group of F then K_k has $\frac{k!}{a}$ subgraphs isomorphic to F. $N_F = \binom{n}{k}\frac{k!}{a} = \frac{(n)_k}{a}$. For cycles, $a = 2k$.

Another Theorem of Erdos: There is a graph, G, with $g(G) \geq n$ and $\chi(G) \geq n$. Another formulation: Given natural numbers $g \geq 3$, $k \geq 2$, $\exists G$, with $|G|k^{3g}$, $g(G) \geq g$ and $\chi(G) \geq k$.

> Fact 1: If $G \in G(n, p)$, $q = 1 - p$ then $Pr[\alpha(G) \geq k] \leq \binom{n}{k}q^{\binom{k}{2}}$ Fact 2: Markov's inequality. Fact 3: Let X be a r.v. representing the number of k-cycles. $E(X) = \frac{(n)_k}{2k}p^k$. Fact 4: If $k > 3$ and $p(n)$ is a function with $p(n) \geq \frac{6kln(n)}{n}$ then $lim_{n\to\infty} Pr[\alpha \geq \frac{n}{2k} = 0$: $\binom{n}{r}q^{\binom{r}{2}} \leq n^n q^{\binom{r}{2}} \leq (ne^{-p\frac{r-1}{2}})^r$ inside expression is $\leq \sqrt{\frac{e}{n}} \to 0$.
>
> Argument: Fix $0 < \epsilon < \frac{1}{k}$, $p = n^{1-\epsilon}$, $X(G)$ is the number of cycles $\leq k$. $E(X) \leq \sum \frac{(n)_i}{2i}p^i \leq \frac{1}{2}(k-2)(np)^k$. $Pr[X \geq \frac{n}{2}] = \frac{E(X)}{\frac{n}{2}} \leq (k-2)n^{k\epsilon-1}$. Pick n big enough so that $Pr[X \geq \frac{n}{2}] > \frac{1}{2}$ and $Pr[\alpha \geq \frac{n}{2k}] < \frac{1}{2}$. So $\exists G$ with $< \frac{n}{2}$ short cycles and $\alpha(G) < \frac{n}{2k}$ delete up to $\frac{n}{2}$ points to eliminate the short cycles producing a graph $H \subseteq G$. $\chi(H) \geq \frac{H}{\alpha(H)} \geq \frac{\frac{n}{2}}{\alpha(G)} > k$.

Definition: ϵ-regular: (A, B) with $X \subseteq A$ and $Y \subseteq B$ such that $|X| \geq \epsilon|A|$ and $|Y| \geq \epsilon|B|$ satisfy $|d(X, Y) - d(A, B)| \leq \epsilon$. ϵ regular partition: (1) $|V_0| < \epsilon|V|$, (2) $|V_i| = |V_1|$, for $i \geq 1$, (3) all but ϵk^2 of the pairs (V_i, V_j) are ϵ regular. *Szemeredi Regularity Lemma:* For every $\epsilon > 0$ and every $m \geq 0$, $\exists M$ such that every graph of order at least m admits an ϵ regular partition $\{V_0, V_1, \ldots, V_k\}$ with $m \leq k \leq M$.

Theorem: There is a *giant component* in $G(n, p)$ when $p = \frac{1+\epsilon}{n}$.

Sunflower Lemma: Let $T = \{S_1, S_2, \ldots, S_k\}$ be a system over a set U, such that (1) $|S_i| \leq l$ and (2) $k > (p-1)^l l!$. Then $\exists F \subseteq T$, $F = \{S_{i_1}, S_{i_2}, \ldots, S_{i_p}\}$ such that $\forall A, B \in F, A \cap B = F$.

Random function statistics: Tail, cycle, predecessor length: $\sqrt{\frac{\pi n}{8}}$, Tree Size: $\frac{n}{3}$, Number of components: $\frac{lg(n)}{2}$, Component Size: $\frac{2n}{3}$.

Sperner's Lemma: A collection F of non-empty subsets of a set X is called an antichain if no set in F is properly contained in another set of F. If $|X| = n$, $|F| \leq \binom{n}{n'}$, where $n' = \lfloor\frac{n+1}{2}\rfloor$. If $|X|$ is even there are exactly 2 maximal antichains, the collection of $\lfloor\frac{n-1}{2}\rfloor$ subsets of X and the collection of $\lfloor\frac{n+1}{2}\rfloor$ subsets

of X. If n is even, there is exactly one maximal antichain, namely, the collection of $\lfloor \frac{n}{2} \rfloor$ subsets of X.

Definitions: Posets, chains (totally ordered subset) and antichains (set in which all subsets are incomparable).

Dilworth's Theorem: The cardinality of a maximal antichain is equal to the minimum number of disjoint chains into which a poset can be partitioned. In a chain of $mn+1$ elements there is a chain of $m+1$ elements or there are $n+1$ incomparable elements.

Symmetry group of Rubik's cube: $|G_R| = 2^{27}3^{14}5^3 7^2 11$.

Some Relations: If $f(x) \in \mathbb{Z} \to x \in \mathbb{Z}$ then $\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor$. $\lfloor \frac{x+m}{n} \rfloor = \lfloor \frac{\lfloor x \rfloor + m}{n} \rfloor$. $\sum_{i=0}^{m-1} \lceil \frac{n-i}{m} \rceil = n$. $\sum_{k=0}^{m-1} \lfloor \frac{nk+x}{m} \rfloor = \sum_{k=0}^{n-1} \lfloor \frac{mk+x}{n} \rfloor$.

Theorem: The following are equivalent: (1) *[Axiom of choice]* If $I \neq \emptyset$ and $\forall i \in I, A_i \neq \emptyset$ then $\prod_{i \in I} A_i \neq \emptyset$; (2) *[Zorn's Lemma]* If $A \neq \emptyset$ is partially ordered and if every chain (including infinite chains!) has an upper bound in A then A contains a maximal element; (3) *[Well ordering]* If $A \neq \emptyset$ has a linear order, $\leq$, then $(A, \leq)$ is has a least element. Transfinite Induction: if $B \subseteq A$ and A is well ordered under $\leq$ and if $\{c \in A : c < a\} \subseteq B \to a \in B$ then $A = B$.

Proof:

$AC \to$ Zorn: Map the partial order into inclusion by $\overline{s}(x) = \{y : y \leq x\}$. $\overline{s} : X \to \mathcal{P}(X)$ and $\overline{s}(x) \subseteq \overline{s}(y)$ iff $x \leq y$. Let $\mathcal{X}$ be the collection of all totally ordered subsets of X. If $\mathcal{C}$ is a totally ordered set (under inclusion) in $\mathcal{X}$ then $\bigcup_{A \in \mathcal{C}} A \in \mathcal{X}$.

Claim: Let $\mathcal{X}$ be a collection of subsets of X such that (1) $Y \subseteq X \in \mathcal{X} \to Y \in \mathcal{X}$ and (2) if $\mathcal{Y}$ is a totally ordered sets in $\mathcal{X}$ then $\bigcup \mathcal{Y} \in \mathcal{X}$. Then there is a maximal set in $\mathcal{X}$.

By the axiom of choice for X, pick an $f : f(A) \in A, A \subseteq X$ and $\forall A \in \mathcal{X}$, put $\hat{A} = A \cup \{f(A)\}$. Further, define $g : \mathcal{X} \to \mathcal{X}$ by $g(A) = A \cup \{f(\hat{A} - A)\}$ if $\hat{A} - A \neq \emptyset$ and $g(A) = A$, otherwise. Note that $\hat{A} - A = \emptyset$ iff A is maximal and that $g(A)$ contains at most one more element than A.

We say $\mathcal{J} \subseteq \mathcal{X}$ is a *tower* if (i) $\emptyset \in \mathcal{J}$, (ii) if $A \in \mathcal{J}$ then $g(A) \in \mathcal{J}$, (iii) if $\mathcal{C}$ is a totally ordered collections of sets in $\mathcal{J}$ then $\bigcup_{A \in \mathcal{C}} A \in \mathcal{J}$.

The intersection of all towers (denoted $\mathcal{J}_0$) is a minimal tower.

We say $C \in \mathcal{J}_0$ is if $A \subseteq C$ or $C \subseteq A$ for all $A \in \mathcal{J}_0$. $\mathcal{J}_0$ is totally ordered iff all sets are comparable. Now fix C.

If $A \in \mathcal{J}_0$, $A \subseteq C$ and $A \neq C$ then $g(A) \subseteq C$ and either $g(A) \subseteq C$ or $C \subseteq g(A), C \neq g(A)$ but $A \subseteq C \subseteq g(A)$ and $A \neq C$ which contradicts the fact that $g(A)$ has only one more element than A. Consider $\mathcal{U} = \{A : A \subseteq C \text{ or } g(C) \subseteq A\}$. We claim $\mathcal{A}$ is a tower. Properties (i) and (iii) are clear. For (ii), there are three cases: if $A \subseteq C, A \neq C$ then $g(A) \subseteq C$; if $A = C$, $g(A) = g(C)$ so $g(A) \in \mathcal{U}$; if $g(C) \subseteq A$, then $g(C) \subseteq g(A)$ and $g(A) \in \mathcal{U}$. Finally, since $\mathcal{J}_0$ is the smallest tower, $\mathcal{J}_0 = \mathcal{U}$. This shows that if C is comparable, so is $g(C)$.

Note that $\emptyset$ is comparable and g maps comparable sets into comparable sets. Thus comparable sets form a tower. Thus $\mathcal{J}_0$ is a totally ordered and $A = \bigcup_{X \in \mathcal{J}_0} X \in \mathcal{J}_0$. $g(A) \subseteq A$ and $A \subseteq g(A)$ so $g(A) = A$ and A is maximal.

Zorn $\rightarrow$ Choice: Given X, consider $f : \text{dom}(f) \subseteq \mathcal{P}(X), \text{range}(f) \subseteq X$ and $f(A) \in A, \forall A \in \text{dom}(f)$. Order these functions by extension. By Zorn, there is a maximal one with $\text{dom}(f) = \mathcal{P}(X) - \{\emptyset\}$.

Theorem: $|P(A)| > |A|$.

Proof: $f : a \mapsto \{a\}$ shows $|P(A)| \geq |A|$. Suppose $|P(A)| = |A|$, then there is a bijection f between $P(A)$ and A. Let $B = \{a : a \notin f(a)\}$. If $b \in B$ and $b \mapsto f(b)$ then $b \notin B$, this is a contradiction.

Schroeder-Bernstein: If A, B are two sets and there are injections $f : A \rightarrow B$ and $g : B \rightarrow A$ then there is a bijection $h : A \rightarrow B$.

Lemma: If there is a subset $A' \subseteq A$ satisfying the hypothesis of the theorem with $A' = B$ then there is a bijection $h : A \rightarrow A'$.
The lemma implies the theorem: Let $A' = g(f(A))$ then by the lemma, $\exists h : A \rightarrow A'$ and $g^{-1} \circ h$ is the desired bijection.
Proof of Lemma: Set $X = \bigcap_{n \geq 0} f^{(n)}(A \setminus A')$ and define $h(x) = f(x), x \in X, h(x) = x, x \notin X$; this is a bijection. First note $f(X) \subseteq X$. If $x, y \in X$ or $x, y \notin X$ it is clear that $h(x) = h(y) \rightarrow x = y$ and by construction, there is no $x \in X, y \notin X$ with $h(x) = h(y)$. If $y \in A'$ and $y \in X$, then $y \in f^{(n)}(A \setminus A')$ for some n in which case $\exists x \in X : h(x) = y$ otherwise $y \notin X$ and $h(y) = y$.

Arrangements: Arrange n objects into k containers. $S(a, b)$- Stirling number of second kind, $p_k(b)$ - number of k partitions of b things.

Objects distinguishable?	Containers distinguishable?	Any	At most one per container	At least one per container
Yes	Yes	n^k	$\frac{n!}{(n-k)!}$	$k!S(n,k)$
No	Yes	$\binom{n+k-1}{n}$	$\binom{n}{k}$	$\binom{n-1}{k-1}$
Yes	No	$\sum_{i=1}^{k} S(n,i)$	1 if $n \leq k$, 0 if $n > k$	$S(n,k)$
No	No	$\sum_{i=1}^{k} p_i(n)$	1 if $n \leq k$, 0 if $n > k$	$p_k(n)$

Select n elements from r distinct objects, with repetition allowed: $\binom{n+r-1}{r}$. Correspondence: $\langle s_0, s_1, \ldots, s_n \rangle \rightarrow \langle s_1 + 0, s_2 + 1, \ldots, s_n + n - 1 \rangle$.]
Number of ways to distribute r non-distinct objects into n distinct cells: $\binom{n+r-1}{(n-1)}$.
Number of ways to distribute r distinct objects into n distinct cells (more than one element in cell allowed): $\frac{(n+r-1)!}{(n-1)!}$.

1.2 Algebra

1.2.1 General Algebra

Solving low degree univariate polynomials: For *quadratic*, $x^2+px+q=0$, $(x_1-x_2)=\sqrt{D}, D=p^2-4q, x_1+x_2=p$. For *cubic*, $az^3+bz^2+cz+d=f(z)$, substitute $z=x-\frac{b}{3a}$ and divide by a to get $x^3+px+q=0$. Put $x=(u+v)$, get $p=3uv$, $q=u^3+v^3$. Following Galois, note $S_3 \supseteq A_3 \supseteq 1$, $(x_1-x_2)(x_1-x_3)(x_2-x_3)=\sqrt{D}, D=-4p^3-27q^2$. After adjoining $\sqrt{D}$, we are left with an irreducible cubic. Put $\rho=-\frac{1}{2}+\frac{1}{2}\sqrt{-3}$ and $(1,x_1)=x_1+x_2+x_3$, $(\rho,x_1)=x_1+\rho x_2+\rho^2 x_3$, $(\rho^2,x_1)=x_1+\rho^2 x_2+\rho x_3$, then $(\rho,x_1)^3=\sum x_i^3-\frac{3}{2}\sum x_i^2x_j+6x_1x_2x_3$. $(\rho,x_1)^3=-\frac{27}{2}q+\frac{3}{2}\sqrt{-3}\sqrt{D}$ and $(\rho^2,x_1)^3=-\frac{27}{2}q-\frac{3}{2}\sqrt{-3}\sqrt{D}$. Solution is: $x=(-\frac{p}{2}+-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}})^{\frac{1}{3}}$. For *quartic*, $az^4+bz^3+cz^2+dz+e=f(z)$, substitute $x=x-\frac{b}{4a}$ and divide by a to get x^4+px^2+qx+r. Again following Galois, $S_4 \supseteq A_4 \supseteq C_4 \supseteq Z_2 \supseteq 1$. $\Theta_1=(x_1+x_2)(x_3+x_4)$ is fixed by C_4 but not A_4. The Θ_i are solutions of $\Theta^3-b_1\Theta^2+b_2\Theta_3-b_3$ with $b_1=2p, b_2=p^2-4r, b_3=-q^2$ and $D=16p^4r-4p^3q^2-128p^2r^2+144pq^2r-27q^4+256r^3$. Look at $(y^2+p)^2=py^2-qy-r$ and pick z to make right hand side $(y^2+p+z)^2=(p+2z)y^2-qy+(p^2-r+2pz+z^2)$ a perfect square.

Fundamental Theorem of Algebra: If $f(z)\in\mathbb{C}[x]$ then $f(z)=0$ has a solution (*root*) in $\mathbb{C}$.

> *Proof:* Let $f(z)=z^n+a_{n-1}x^{n-1}+...+a_0$ and $\mu=\inf(|f(z)|)$. If $\mu=0$, we're done since the minimum must occur in bounded ball. So assume $\mu\neq 0$. Let the minimum occur at z_0 and put $f(z_0)=w_0$, $w=f(z_0+\zeta)$. $\frac{w}{w_0}=1+q\zeta^\nu(1+\zeta\xi)=1-h\rho^\nu(1+\zeta\xi)$ where $\zeta=\rho(cos(\theta)+isin(\theta))$ and $q=h(cos(\lambda)+isin(\lambda))$. So we can find a point with smaller modulus than w_0. This contradicts the assumed minimality at z_0.

Facts about roots of unity: Consider $f(x)=x^h-1$ over F where $(char(F),h)=1$ or $char(F)=0$. The roots of f form an abelian group, G. $x\in G\to |x| \mid |G|$. Since $(f,f')=1$ there are h distinct roots, set $h=\prod_{i=1}^m q_i^{v_i}$. $\{x: x^{h/q_i}=1\}$ is a group of order h/q_i so $\forall i, \exists x_i\in G: x^{h/q_i}\neq 1$. Setting $b_i=x_i^{h/{q_i}^{v_i}}$, then $\chi=\prod b_i$ has order exactly h and is a primitive hth root of unity. Let the number of such roots be $\varphi(h)$; if $(r,s)=1, \varphi(rs)=\varphi(r)\varphi(s)$ so $\varphi(\prod_i {q_i}^{v_i})=\prod_i \varphi({q_i}^{v_i})=\prod_i({q_i}^{v_i}-{q_i}^{v_i-1})=h\prod_i(1-\frac{1}{q_i})$. Set $n=\varphi(h)$ and $\Phi_n(x)=\prod_i(x-\psi_i)$ where ψ_i are the primitive roots. $x^h-1=\prod_{d|h}\Phi_d(x)$ and by Moebius inversion, $\Phi_h(x)=\prod_{d|h}(x^d-1)^{\mu(\frac{h}{d})}$.

Theorem: $\Phi_h(x)$ is irreducible of degree $\varphi(h)$.

> *Proof:* Let $\zeta\in\mathbb{C}$ be a primitive root of $\Phi_h(x)$ with minimal polynomial $f(x)$ and $(p,h)=1$. Let $g(x)$ be the minimal polynomial for ζ^p so $g(\zeta^p)=0$. $x^h-1=f(x)g(x)h(x)$ and $g(x^p)=f(x)k(x)$. $g(x^p)=g(x)^p \pmod p$. If $\phi(x)\mid f(x)$ then $\phi(x)\mid g(x)^p \pmod p$. So $\phi(x)^2\mid x^h-1$ but this contradicts the fact that x^h-1 does not have roots of multiplicity 2. It follows that if $(p_i,h)=1$, $\zeta^{p_1p_2\cdots p_k}$ is a primitive root and the degree of $f(x)$ is $\varphi(h)$.

Note this shows that $Aut(\mathbb{Q}[\zeta])\cong\mathbb{Z}_h^*$. So if $h=q=p^n$, the Galois group is cyclic and the subfields correspond to the cyclic subgroups of $\mathbb{Z}_q^*$. The qth roots of 1 are expressible as radicals if $char(F)=0$ or $char(F)>q$. If $N_p(d)=$ number of irreducible monic polynomials of degree d in $GF(p)[x]$ then $p^n=\sum_{d|n}dN_p(d)$ and $N_p(d)=\frac{1}{n}\sum_{d|n}\mu(\frac{n}{d})p^d$. $x^{p^n}-x=\prod_{f,irred,monic,deg(f)|n}f$.

Eisenstein's Criteria: If $f(x)=\sum_{i=0}^n a_nx^n$, $a_n\neq 0 \pmod p$, $a_i=0 \pmod p, i<n$ and $a_0\neq 0 \pmod{p^2}$ then f is irreducible.

Factoring in finite number of steps: Let $g(x)\in\mathbb{Z}[x]$ if $f(x)\mid g(x)$ then $f(n)\mid g(n)$ for all n.

$deg(f) = s \leq \lfloor \frac{deg(g)}{2} \rfloor$. Pick s integers i_j and use the integer factors of $g(i_j)$ to get possible $f(i_j)$; there are a finite number of ways to pick the factors. For each possibility, we can solve for the s coefficients of f.

1.2.2 Free groups, rings and modules

Theorem: Every group is the homomorphic image of a free group.

> *Proof:* Let F be the elements of G and R be the relations $abc^{-1} = 1$. G is the free group on the symbols F with relations R.

Theorem: If $x_1, x_2, \ldots, x_n$ is a basis for a free abelian group for a free abelian group and $y_i = \sum_{j=1}^{n} a_{ij}x_j$ with $a_{ij} \in \mathbb{Z}$ then $\langle y_i \rangle$ is a basis iff $det(a_{ij}) = \pm 1$.

> *Proof:* Since $\langle y_i \rangle$ is a basis, $x_i = \sum_j b_{ij}y_j$ for some $b_{ij} \in \mathbb{Z}$. Let $A = (a_{ij})$ and $B = (b_{ij})$ then $BA = I$ and $det(B) = det(A) \in \mathbb{Z}$, so $det(A) = \pm 1$. $\langle y_i \rangle$ is a basis iff $det(a_{ij}) = \pm 1$.

Theorem: Every subgroup $H \leq G$ of a free abelian group G of rank n is free abelian group of rank $s \leq n$. Moreover, $\exists u_1, \ldots, u_s \in G$ and $\alpha_1, \ldots, \alpha_s \in \mathbb{Z}$ such that $\alpha_1 u_1, \ldots, \alpha_s u_s$ is a basis of H.

> *Proof:* By induction on n. True for $n = 1$. Pick a basis $w_1, \ldots, w_n$ of G and for $h \in H : h = h_1w_1 + \ldots + h_nw_n$. Let $\alpha_1 \neq 0$ be the smallest (in absolute value) coefficient in any such sum and assume WLOG it occurs as the coefficient of w_1 for some h. Let $v_1 = \alpha_1 w_1 + \beta_2 w_2 + \ldots + \beta_n w_n \in H$. $\exists q_i, r_i : \beta_i = \alpha_1 q_i + r_i$. Put $u_1 = w_1 + q_2 w_2 + \ldots + q_n w_n$ then $u_1, w_2, \ldots, w_n$ is another basis for G and $v_1 = \alpha_1 u_1 \in H$. Now put $H' = \{h = m_2 w_2 + \ldots + m_n w_n : h \in H\}$. $H' \cap (v_1) = 0$ and $H = H' \oplus (v_1)$.

Theorem: If G is a free abelian group of rank r and $H \leq G$ then G/H is finite iff H has rank r. If G has basis $x_1, \ldots, x_s$ and H has basis $y_1, \ldots, y_s$ with $y_i = \sum_{j=1}^{s} a_{ij}x_j$ then $|G/H| = det(a_{ij})$.

> *Proof:* By the structure theorem, viewing G as a $\mathbb{Z}$-module, $G \approx \mathbb{Z}^s/H$. In the diagonal form, the order of the direct sums appears on the diagonal and the product is $det(a_{ij})$.

Theorem: Every finitely generated abelian group with n generators is the direct product of a free abelian group and a finite abelian group.

> *Proof:* Let $G = \langle x_i, \ldots, x_n \rangle$ and $H = \{x \in G : x^n = 1, n \in \mathbb{Z}\}$. G/H is free and finitely generated. Apply the theorem (just before the structure theorem) to $g \to G/H$ to conclude the proof.

Calculating with free groups: Let F_m be a free abelian group generated by $a_1, a_2, \ldots, a_m$ and define $E_i = r_{i1}a_1 + r_{i2}a_2 + \ldots + r_{im}a_m$ where $r_{ij} \in \mathbb{Z}$ and $1 \leq i \leq n$; further, put $b_i = E_i$ and let $K = \langle b_i \rangle$. Suppose G is the free abelian group generated by a_i subject to $E_i = 0$. Then $G \cong F_m/K$. Let R represent the matrix (r_{ij}) then (1) if the matrix $S = (s_{ij})$ is obtained from R by elementary row operations then $c_i = s_{i1}a_1 + \ldots + s_{im}a_m \in K$; and, (2) if the matrix $S = (s_{ij})$ is obtained from R by elementary column operations then $\exists a'_i \in F_m : b_i = s_{i1}a'_1 + \ldots + s_{im}a'_m$ (so the a'_i generate K). By applying elementary row and column operations, we can transform R into the diagonal matrix $D = diag(d_1, d_2, \ldots, d_r, 0, \ldots, 0)$ where $d_i \mid d_{i+1}$ and $G \cong \mathbb{Z}/(d_1) \times \mathbb{Z}/(d_2) \times \ldots \times \mathbb{Z}/(d_r) \times \mathbb{Z} \times \ldots \times \mathbb{Z}$ where there are $m - r$ copies of $\mathbb{Z}$ in the product.

Definition: If $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_i \in R$, a UFD, the *content* of f is $cont(f) = gcd(a_0, a_1, \ldots, a_n)$.

Gauss' Lemma: If D is a UFD and $f, g \in D[x]$ then $cont(f(x)g(x)) = cont(f(x))cont(g(x))$. If $f(x) \in R[x], deg(f) > 0$ and $f(x)$ is irreducible in $R[x]$ then it is irreducible in $K[x]$.

Proof: Suffices to show that if $cont(f) = cont(g) = 1$ then $cont(fg) = 1$. Let $f(x) = a_0 + a_1x + \ldots + a_nx^n$ and $g(x) = b_0 + b_1x + \ldots + b_mx^m$ with $a_i, b_i \in R$. Suppose, by way of contradiction that $p \mid cont(fg)$. Let i be maximal subject to $p \nmid a_i$ and j be maximal subject to $p \nmid b_j$. The coefficient of x^{i+j} in fg is $c_{i+j} = \sum_{k=0}^{i+j} a_k b_{i+j-k}$. $p \mid a_k, k < i$ and $p \mid b_{i+j-k}, k > i$ but $p \nmid a_i b_j$ so $p \nmid c_{i+j}$.

Theorem: If R is a UFD then $R[x]$ is a UFD.

Proof: Let the field of quotients of R be K. If $f(x) \in R[x]$, $f(x) = cont(f)f'(x)$ with $cont(f') = 1$. By Gauss' lemma, it suffices to prove the result when f is primitive. $f(x) = f_1(x) \cdot f_2(x) \ldots \cdot f_n(x)$ over K with each f_i irreducible; further, this factorization is unique up to units in K. So $\exists c_i, d_i \in R$ such that $d_i f_i(x) = c_i p_i(x)$ where $p_i \in R[x]$ satisfies $cont(p_i) = 1$. Put $c = \prod_{i=1}^n c_i$ and $d = \prod_{i=1}^n d_i$ then $df(x) = cp_1(x) \cdot p_2(x) \ldots \cdot p_n(x)$ so c and d are units of R by Gauss. This shows a factorization exists. If $f(x) = dq_1(x) \cdot q_2(x) \ldots \cdot q_m(x)$ is another such factorization then $m = n$ and $p_i = u_i q_j$, $u_i \in K$ by the factorization result in $K[x]$. Thus $t_i p_i = r_i q_j$, $r_i, t_i \in R$ with $(t_i, r_i) = 1$. By Gauss, $t_i = u_i r_i$ where u_i is a unit in R. Finally, d is a unit in R again by Gauss's lemma and the proof is complete.

Ring theoretic Chinese Remainder Theorem: If $I_j, j = 1, 2, \ldots, n$ are ideals of R and $I_j + I_k = R$ for $j \neq k$, then $\forall x_1, x_2, \ldots, x_n \in R, \exists x \in R$ such that $x = x_j \pmod{I_j}$.

Corollaries: Under the same assumptions as the theorem, $\psi : R \to R/I_1 \times R/I_2 \times \ldots \times R/I_n$ given by $x \mapsto x \pmod{I_1} \times \ldots \times x \pmod{I_n}$ is surjective and $R/(\bigcap_{j=1}^n I_j) \cong R/I_1 \times R/I_2 \times \ldots \times R/I_n$. If $m = \prod_{i=1}^n p_i^{r_i}$, $\mathbb{Z}/(m\mathbb{Z}) \cong \prod_i \mathbb{Z}/({p_i}^{r_i}\mathbb{Z})$ and $\psi(m) = \prod_i \psi({p_i}^{r_i})$. If R is cyclic of order n then $End(R) \cong \mathbb{Z}/(n\mathbb{Z})$ and $(\mathbb{Z}/(n\mathbb{Z}))^* \cong Aut(R)$.

Hilbert Basis Theorem: If R is a ring with identity such that every ideal is finitely generated then $R[x]$ has the same property.

Proof: Let I be an ideal of $R[x]$ and I_j be the set of coefficients of the x^j terms in I. I_j is an ideal of R and $I_j \subseteq I_{j+1}$. Since R is finitely generated, $\exists m : I_j \subseteq I_m, \forall i$. Let the generators of I_j be $\langle b_j^{(1)}, b_j^{(2)}, \ldots, b_j^{(i_j)}, \rangle$. So there are polynomials $f_j^{(i)}(x) \in I_j$: $f_j^{(i)}(x) = b_j^i x^j + g_j^{(i)}(x), deg(g_j^{(i)}(x) < j)$. The polynomials

$$\langle f_0^{(1)}(x), f_0^{(2)}(x), \ldots, f_0^{(i_0)}(x), f_1^{(1)}(x), f_1^{(2)}(x), \ldots, f_1^{(i_1)}(x), \ldots, f_m^{(1)}(x), f_m^{(2)}(x), \ldots, f_m^{(i_m)}(x)\rangle$$

generate I.

Groups with operators (M) and invariant subgroups: Projection commutes with all inner automorphisms; such an endomorphism is called normal. An $M-$group G is decomposable iff there are projections. Any $M-$group satisfying DCC is a direct product of a finite number of indecomposable $M-$groups. If $\eta \in End(G)$ then $\sqrt{\eta} = \{z \in G : z\eta^s = 1\}$.

Fitting Lemma: Let G be an $M-$group that satisfies ACC and DCC and η is a normal endomorphism of G then $G = \sqrt{\eta} \times H$ and $H\eta = H$. If G is an indecomposable $M-$group satisfying ACC and DCC then any normal $M-$endomorphism of G is either **nilpotent** or an automorphism. Suppose η_1, η_2 are normal nilpotent $M-$endomorphisms, if $\eta_1 + \eta_2$ is an endomorphism it is nilpotent. **Krull-Schmidt** follows from this.

Definition: M is *unitary* if $RM = M$.

Primary decomposition: If A, B are ideals, we say $A \mid B$ if $B \subseteq A$. Q is *primary* iff $ab = 0 \pmod{I} \rightarrow a = 0 \pmod{Q}$ or $b \in \sqrt{I}$. If Q is primary then $\sqrt{Q}$ is prime. Every irreducible ideal in a Noetherian ring is primary. Every ideal in a Noetherian ring is the finite intersection of primary ideals. If Q_1, Q_2 are primary and $\sqrt{Q_1} = \sqrt{Q_2}$ then $Q_1 \cap Q_2$ is primary. If $Q_1 \cap Q_2 \cap \ldots \cap Q_r = Q_1' \cap Q_2' \cap \ldots \cap Q_s'$ are two irredundant representations into primary ideals whose associated primes are distinct, then $r = s$ and the set of associated primes is identical. If $R^2 = R$ is a commutative ring then every maximal ideal is prime. Let P be a prime ideal of R $(1 \in R)$ then (1) There is a 1-1 correspondence between the set of prime ideals of R contained in P and (2) the prime ideals of R_P given by $\mathbb{Q} \mapsto \mathbb{Q}_P$. A local ring is a commutative ring with identity containing a unique maximal ideal. If R is a commutative ring with identity, the following are equivalent: (1) R is a local ring; (2) all non-units of R are contained in an ideal $M \neq R$; (3) the non-units form an ideal. Substitution from a the polynomial ring to the ring of coefficients is a homomorphism.

Theorem: If R is Noetherian and $a \in M$ is $R-$*integral* iff $\exists$ a finitely generated submodule of M that contains all powers of a. The totality G of elements of M that are $R-$integral is a subring of M containing R. The ring G or $R-$integral elements is integrally closed in R.

> *Proof:* $\rightarrow$. Suppose $a^n + r_{n-1}a^{n-1} + \ldots + r_0 = 0$. Put $M = \langle a^{n-1}, \ldots, 1\rangle$. $a^k \in M, \forall k$. $\leftarrow$. Consider $\langle 1\rangle \subseteq \langle 1, a\rangle \subseteq \langle 1, a, a^2\rangle \subseteq \ldots$. Since R is noetherian, this series is finite. Say $M = \langle 1, a, a^2, \ldots, a^m\rangle$ is the terminal module in the series. $a^k \in M, \forall k$.

Projective and injective modules: If A, B, C, A', B', C' are modules over a ring R with identity and we have the diagrams $0 \rightarrow A \xrightarrow{\mathrm{f}} B \xrightarrow{\mathrm{g}} C \rightarrow 0$ and $0 \rightarrow A' \xrightarrow{\mathrm{f}'} B' \xrightarrow{\mathrm{g}'} C' \rightarrow 0$ with $A \xrightarrow{\alpha} A'$, $B \xrightarrow{\beta} B'$, and $C \xrightarrow{\gamma} C'$, then (1) β is a monomorphism if α and β are and (2) β is a epimorphism if α and β are. P is projective if given A, B, g, f and morphism diagrams: $A \xrightarrow{\mathrm{g}} B \rightarrow 0$ and $P \xrightarrow{\mathrm{f}} B$, $\exists h, P \xrightarrow{\mathrm{h}} B$ which makes the diagram commute. J is injective if given A, B, g, f and morphism diagrams: $A \xrightarrow{\mathrm{g}} B \rightarrow 0$ and $A \xrightarrow{\mathrm{f}} J$, $\exists h, B \xrightarrow{\mathrm{h}} J$ which makes the diagram commute. Every free module F over R with identity is projective. If R is a ring with identity, TFAE: (1) P is projective, (2) every short exact sequence $0 \rightarrow A \xrightarrow{\mathrm{f}} B \xrightarrow{\mathrm{g}} P \rightarrow 0$ splits so $B = P \oplus A$ and (3) $\exists F$, free such that $F = K \oplus P$. If R is a ring with identity, TFAE: (1) J is injective, (2) every short exact sequence $0 \rightarrow A \xrightarrow{\mathrm{f}} B \xrightarrow{\mathrm{g}} C \rightarrow 0$ splits so $B = J \oplus C$ and (3) J is a direct summand. $0 \rightarrow A \xrightarrow{\psi} B \xrightarrow{\phi} C$ is exact if: $0 \rightarrow Hom(D, A) \xrightarrow{\psi} Hom(D, B) \xrightarrow{\phi} Hom(D, C)$ is. $A \xrightarrow{\theta} B \xrightarrow{\zeta} C \rightarrow 0$ is exact if: $0 \rightarrow Hom(A, D) \xrightarrow{\psi} Hom(B, D) \xrightarrow{\phi} Hom(C, D)$ is. The full short exact sequence is split exact iff the corresponding dual (Hom) sequence is.

Integral closure of UFD's: If A us a unique factorization domain, A is integrally closed. The integral closure in a number field K is called the ring of algebraic integers. Algebraic integers form a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

Results on trace and norm: Let $[E : F] = n$ and $[F(x) : F] = d$ and $x_1, x_2, \ldots, x_d$ be the roots of $min_F(x)$ then $N_{E/F}(x) = (\prod_{i=1}^{d} x_i)^{\frac{n}{d}}$ and $Tr_{E/F}(x) = \frac{n}{d}(\sum_{i=1}^{d} x_i)$. If E/F is separable then $N_{E/F}(x) = \prod_{i=1}^{n} \sigma_i(x)$ and $Tr_{E/F}(x) = \sum i = 1^n \sigma_i(x)$. If $F \subseteq E \subseteq K$ then $N_{E/F}(N_{K/E}(x)) = N_{K/F}(x)$ and $Tr_{E/F}(Tr_{K/E}(x)) = Tr_{K/F}(x)$. If E/F is a finite separable extension, $\exists x \in E : Tr_{E/F}(x) = 0$ and $(x, y) \rightarrow Tr_{E/F}(xy)$ is bilinear. For this paragraph, L be a separable extension of K, $A \subseteq K$ be a ring of integers and $B \subseteq L$ be a ring of algebraic integers. $\vec{x}$ is a basis for L/K iff $\Delta(\vec{x}) \neq 0$. If $L = K(x)$ and f is a minimal polynomial of x over K then $\Delta(1, x, x^2, \ldots, x^{n-1}) = disc(f) = \prod_{i<j}(x_i - x_j) = (-1)^{\binom{n}{2}} N_{L/K}(f'(x))$. There is a basis for L/K consisting of elements of B. If A is a PID then B is a free A-module of rank $[L : K]$. If $a_i \in A$ then $(x_1 - a_1, x_2 - a_2, \ldots, x_n - a_n)$ is a maximal ideal.

Theorems on chain conditions: Let M be an R module. The following are equivalent (1) M satisfies *ACC (Noetherian)*, (2) Any non empty collection of submodules of M has a maximal element. The following are equivalent (1) M satisfies *DCC (Artinian)*, (2) Any non empty collection of submodules of M has a minimal element. M is Noetherian iff every submodule is finitely generated. M is Artinian iff every submodule is finitely co-generated.

Example of Noetherian ring: PIDs, $F[x]$. $F[x_1, x_2, \ldots]$ is *neither* Noetherian nor Artinian. If $N \subseteq M$ then M is Noetherian iff N and M/N are. M has a composition series iff M is Noetherian and Artinian. L be a separable extension of K, $A \subseteq K$ be a ring of integers $B \subseteq L$ be a ring of algebraic integers, if A is integrally closed in K and A is Noetherian, so is B. Let P be a prime ideal of R and $P \supseteq I_1 I_2 \ldots I_n$ then $\exists k : P \supseteq I_k$. Let I be a non-zero ideal of a noetherian integral domain R then $I \supseteq P_1 P_2 \ldots P_n$ for P_i prime. Let R be a non-zero ideal of a noetherian integral domain and K its field of quotients, I is a fractional ideal if I is an R-module and $\exists r \in R : rI \subseteq R$. If I is a finitely generated R submodule of K then I is a fractional ideal. If R is Noetherian and I is a fractional ideal of R then I is a finitely generated R submodule of K.

Definition: A *Dedekind Domain ("DD")* is an integral domain, R, such that (1) R is Noetherian, (2) R is integrally closed, and, (3) Every non-zero prime ideal of R is maximal. PIDs are DDs. Algebraic integers in a number field is a DD. If P is a non-zero prime ideal in a DD, R and $J = \{x \in K : xI \subseteq R\}$ then (1) $R \subseteq J$ and (2) J is a fractional ideal and $PJ = R$. If I is a fractional ideal in a DD, R then $I = \prod_{i=1}^{N} P_i^{n_i}$ ($n_i \in \mathbb{Z}$ not just $\mathbb{Z}^{\geq 0}$), $n_P(I) = n_i$. The fractional ideals form a group. A non-zero fractional ideal is integral iff all n_i in the forgoing representation are ≥ 0. $I_1 \supset I_2$ iff $\forall P, n_P(I_1) \leq n_P(I_2)$. If I_1, I_2 are integral ideals then $I_1 \mid I_2$ if $I_2 = JI_1$. $I_1 \mid I_2$ iff $I_1 \supseteq I_2$. L be a separable extension of K, $A \subseteq K$ be a ring of integers, if A is a DD, B is a DD. An abelian group with a basis of n elements is a *free abelian group* of rank n.

Kummer's idea: For a field, K let $\mathfrak{D}_K$ denote the ring of integers in K. Start with K and extend it to L such that $\mathfrak{D}_K \subseteq \mathfrak{D}_L$. For example, $K = \mathbb{Q}(\sqrt{15}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5}) = L$. $10 = \sqrt{5}\sqrt{5}(\sqrt{5} + \sqrt{3})(\sqrt{5} - \sqrt{3})$. Let $I = (\sqrt{5} + \sqrt{3}) \cap \mathfrak{D}_K$. $(\sqrt{15} + 3) \in I$, $(\sqrt{15} + 5) \in I$ so $2 \in I$ and I is not principal.

Definition: A $\mathfrak{D}$-submodule $\mathfrak{a}$ of K is a *fractional* ideal of $\mathfrak{D}$ if $\exists c \in \mathfrak{D} : c\mathfrak{a} \subseteq \mathfrak{D}$ and $c\mathfrak{a} = \mathfrak{b}$ is an ideal of $\mathfrak{D}$. An ideal $\mathfrak{p}$ is prime if $\mathfrak{p} \mid \mathfrak{ab}$ implies $\mathfrak{p} \mid \mathfrak{a}$ or $\mathfrak{p} \mid \mathfrak{b}$. $\mathfrak{a}^{-1} = \{x \in K : x\mathfrak{a} \subseteq \mathfrak{D}\}$.

Theorem: If a domain is *noetherian* the elements factor into irreducibles. If every irreducible in a domain, D, is prime then D is a UFD.

Proof:
Claim 1: Let $\mathfrak{a} \neq 0$, $\exists \mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ such that $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_n \subseteq \mathfrak{a}$.
Claim 2: $\mathfrak{a}^{-1}$, exists.
Claim 3: If $\mathfrak{a}$ is a proper ideal then $\mathfrak{a} \not\supseteq \mathfrak{D}$.
Claim 4: If $\mathfrak{a}S \subseteq \mathfrak{a}$ for $S \subseteq K$ then $S \subseteq \mathfrak{D}$.
Claim 5: If $\mathfrak{p}$ is a maximal ideal then $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{D}$.
Claim 6: If $\mathfrak{a}$ is a fractional ideal, it has an inverse and $\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{D}$.
Claim 7: Every non-zero ideal $\mathfrak{a}$ is a product of prime ideals.
Claim 8: Prime factorization is unique.

Theorem: The non-zero fractional ideals of $\mathfrak{D}$ form a group and the identity is $\mathfrak{D}$. Every non-zero ideal of $\mathfrak{D}$ can be written as a product of prime ideals uniquely up to the order of factors.

Proof: Todo.

Definition: $N(\mathfrak{a}) = \mathfrak{D}/\mathfrak{a}$.

Theorem: Let G be an additive subgroup of $\mathfrak{D}$, a ring of algebraic integers, of rank n equal to the degree of an algebraic number field K with $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ then $|\mathfrak{D}/G|^2 \mid \Delta(\alpha_1, \ldots, \alpha_n)$.

Proof: Todo.

Chain conditions and exact sequences: If $0 \to A \xrightarrow{f} B \xrightarrow{g} P \to 0$, B satisfies ACC (resp DCC) iff A and C do. A satisfies ACC on submodules iff each submodule is finitely generated (same for rings). Jordan-Holder for modules (composition series have unique refinements). A has a composition series iff A satisfies ACC and DCC. If D is a division ring then $Mat_{n\times n}(D)$ is both Noetherian and Artinian. An ideal $P(\neq R)$ in a commutative ring R is prime iff $R - P$ is a multiplicative set. If S is multiplicative and $S \cap I \neq \emptyset$, $\exists P$, prime that is maximal with respect to the disjoint property. $rad(I) = \{r \in R : r^n \in I\}$.

Theorem: Every transcendental extension has a *transcendence basis.* If $\langle x_1, x_2, \ldots, x_n\rangle$ spans E algebraically and $S \subseteq E$ is algebraically independent then $|S| \leq n$. (Use Steinmetz replacement.)

Noetherian Normalization Lemma: Let R be an integral domain which is a finitely generated extension of K and suppose r is the transcendence degree over K of the quotient field of R, then $\exists t_1, \ldots, t_r$ algebraically independent elements such that R is integral over $K[t_1, \ldots, t_r]$.

Localization: Let S be a multiplicative subset of R and $h : a \mapsto a/1$ be the natural map. If J is an ideal in $S^{-1}R$ then $S^{-1}J = I$ is an ideal of R and $I \subseteq h^{-1}(S^{-1}(I)$ with equality if $I \cap S = \emptyset$. If I is a prime ideal of R and $I \cap S = \emptyset$ then $S^{-1}R$ is a prime ideal of $S^{-1}R$. If P is a prime ideal of R and $S = R - P$ is a multiplicative set, denote $S^{-1}R$ as R_P. R_P has a unique maximal ideal consisting of non-units of R_P. $\sqrt{I} = P_1 \cap P_2 \cap \ldots \cap P_k$ for some prime ideals P_i.

1.2.3 Polynomials

Basic Symmetric polynomials: $\sigma_1 = \sum x_i$, $\sigma_2 = \sum x_i x_j$, etc. Every symmetric function $f(x_1, \ldots, x_n) = (z - x_1)\ldots(z - x_n)$ can be written as a polynomial with coefficients in the basic symmetric polynomials.

Proof 1: Let $a{x_1}^{a_1}{x_2}^{a_2}\ldots{x_n}^{a_n}$ be the leading coefficient of a symmetric form in lexicographic order, subtracting $a{\sigma_1}^{a_1-a_2}{\sigma_2}^{a_2-a_3}\ldots{\sigma_n}^{a_n}$ leaves a symmetric form with leading coefficient smaller in lexicographic order.
Proof 2: By induction on the weight. True for 1. If $f(x_1, \ldots, x_n)$ is symmetric, so is $\frac{f(x_1,\ldots,x_{n-1},0)}{z}$. So $\frac{f(x_1,\ldots,x_{n-1},0)}{z} = \phi((\sigma_1)_0, \ldots, (\sigma_{n-1})_0)$ Set $f_1(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) - \phi((\sigma_1)_0, \ldots, (\sigma_{n-1})_0)$. $f_1(x_1, \ldots, x_{n-1}, 0) = 0$ so x_n and hence σ_n divides f_1 thus $f_1 = \sigma_n g$ and g is writable as a polynomial in the basic symmetric functions by induction so $f(x_1, \ldots, x_n) = \sigma_n\psi(\sigma_1, \ldots, \sigma_n) + \phi(\sigma_1, \ldots, \sigma_{n-1})$. Further, the representation is essentially unique which you can show by proving $\phi(y_1, \ldots, y_n) \neq 0 \to \phi(\sigma_1, \ldots, \sigma_n) \neq 0$ (Prove).

Theorem: Let $\sigma_1, \ldots, \sigma_n$ be the symmetric functions on n variables. $\varphi(\sigma_1, \ldots, \sigma_n) = 0$ iff $\varphi(x_1, \ldots, x_n) = 0$.

Proof: Proof by induction on n. Trivial for $n = 1$. Let $\phi(y_1, \ldots, y_n) = \phi_k(y_1, \ldots, y_{n-1})y^m + \ldots + \phi_0(y_1, \ldots, y_{n-1})$ be a counterexample of minimum degree in y_n. Then $\phi(\sigma_1, \ldots, \sigma_n) = \phi_k(\sigma_1, \ldots, \sigma_{n-1})\sigma^m + \ldots + \phi_0(\sigma_1, \ldots, \sigma_{n-1}) = 0$. Put $x_n = 0$. Then $\phi_0(\sigma_1, \ldots, \sigma_{n-1}) = 0$ but $\phi_0(y_1, \ldots, y_{n-1}) \neq 0$ which contradicts the induction hypothesis.

Resultant: If $f_v(x) = v_n x^n + \ldots + v_0$ and $g_w(x) = w_m x^m + \ldots + w_0$, $\exists \phi_{v,w}(x), \psi_{v,w}(x) : \phi_{v,w}(x) f_v(x) + \psi_{v,w}(x) g_u(x) = R(v,w) = v_m^n w_n^m \prod_{i<j}(t_i - u_j)$, where t_i, u_j are roots of f, g respectively. Resultant is 0 iff equations have common solution. Consider the equations written in matrix notation:

$$\begin{pmatrix} x^{m-1}f_v(x) \\ x^{m-2}f_v(x) \\ \ldots \\ f_v(x) \\ x^{n-1}g_w(x) \\ x^{n-2}g_w(x) \\ \ldots \\ g_w(x) \end{pmatrix} = \begin{pmatrix} v_n & v_{n-1} & \ldots & v_0 & 0 & 0 & \ldots & 0 \\ 0 & v_n & v_{n-1} & \ldots & v_0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & v_n & v_{n-1} & \ldots & v_0 \\ w_m & w_{m-1} & \ldots & w_0 & 0 & 0 & \ldots & 0 \\ 0 & w_m & w_{m-1} & \ldots & w_0 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & w_m & w_{m-1} & \ldots & w_0 \end{pmatrix} \begin{pmatrix} x^{n+m-1} \\ x^{n+m-2} \\ \ldots \\ \ldots \\ \ldots \\ \ldots \\ x \\ 1 \end{pmatrix}$$

Proof: Let the column vectors be $C_{m+n-1} \ldots C_0$. $C = (x^{m-1}f_v(x), \ldots, g_w(x))^T$. $C = C_{m+n-1} \cdot x_{m+n-1} + \ldots + 1 \cdot C_0$. Now solve for 1. $1 = \frac{det(C_{m+n-1}, \ldots C_1, C)}{det(C_{m+n-1}, \ldots C_1, C_0)}$. Get $\phi_{v,w}(x) f_v(x) + \psi_{v,w}(x) g_w(x) = R(v,w)$.

Theorem: Let $f_1, \ldots, f_s$ be polynomials of one variable with indeterminate coefficients. $\exists d_1, d_2, \ldots, d_h$ of integral polynomials in the coefficients of f_i such that if the coefficients are assigned values (*"specialized"*) from k, $d_i = 0$ iff either the $f_i = 0$ have a common solution or the leading coefficients vanish.

Proof: Set $f_u = u_1 f_1 + \ldots + u_s f_s$, $f_v = v_1 f_1 + \ldots + v_s f_s$. $(f_u, f_v) = 1$ iff $(f_1, f_2 \ldots, f_s) = 1$. $R(f_u, f_v) = 0$ iff f_u and f_v have a non-trivial common factor. But $R(f_u, f_v)$ is a polynomial in u_i, v_j with coefficients which are integral in the coefficients of f_i. Arrange these in the order of powers of $u_i v_j$. These are the d_i. The proof also shows that $d_i = 0 \,(\mathrm{mod}\ (f_1, f_2, \ldots f_r))$ and $(d_1, d_2 \ldots d_l) = 0 \,(\mathrm{mod}\ (f_1, f_2, \ldots f_r))$.

Theorem: If $f_1, \ldots, f_r \in F[x_1, \ldots, x_n]$ has no common zeros, $\exists A_1, \ldots A_r$ such that $\sum_i A_i f_i = 1$.

Proof: By the induction on number of variables. True for $n = 1$ by usual theory of polynomials over fields. Assume it's true for $n - 1$. Let $\overline{f}_i(x) = f_i(x, x_2, \ldots, x_n) = \sum_{j-0}^{n_i} g_{ij}(x_2, \ldots, x_n) x^j$. The $\overline{f}_i$ have no common solution or the f_i would; thus by the previous result, regarding the coefficients of x^j as indeterminants, $\exists d_{lk}$ which are not simultaneously 0 [or again, the f_i would have a common solution], such that $\sum_{lk} B_{lk} d_{lk} = 1$. After substitution, $\sum_{ij} C_{ij} g_{ij} = 1$. Further, $g_{ij} = \sum_j A_j f_j$, again by the previous result. After substituting again, we get $\sum_j D_j f_j(x, x_2, \ldots, x_n)$ which is what we want.

Nullstellensatz: If $f(x_1, \ldots, x_n) \in F$ vanishes at all the common zeros of $f_1(x_1, \ldots, x_n), \ldots, f_r(x_1, \ldots, x_n)$ in every extension of F, then $f^k(x_1, \ldots, x_n) \in (f_1(x_1, \ldots, x_n), \ldots, f_r(x_1, \ldots, x_n))$ for some k.

To prove this, look at $f_1, \ldots, f_r, 1 - zf$, put $z = \frac{1}{f}$ and clear denominators. Note that if $h_1, \ldots, h_m$ are zero for all common zeros of the f_i, $(h_1, \ldots, h_m)^\rho = 0 (f_1, f_2, \ldots, f_r)$.

Note that an algebraic condition for solvability is not always possible: Consider $a_1 x_1 + a_2 x_2 + a_3 = 0$, $b_1 x_1 + b_2 x_2 + b_3 = 0$; they have a solution in general if $a_1 b_2 - b_1 a_2 \neq 0$ and the d_i (the resultant system) would have to vanish for indeterminant a, b and the equation would always have a solution but it doesn't. However, this does work for homogeneous equations (forms).

General idea of *elimination* for forms relies on three lemmas:

Lemma 1: We can assume x_1 appears with non-zero constant coefficient.

Proof: if not, substitute $x_1 = u_1 x_1'$, $x_2 = x_2' + u_2 x_1'$, ..., $x_n = x_n' + u_n x_1'$.

Lemma 2: If $\mathcal{F}$ has a non-trivial common solution, the d_i do too.

Proof: If the coefficients do not vanish, the d_i give rise to a solution $(\xi_2, \ldots, \xi_n)$ in $(x_2, \ldots, x_n)$ which can be extended to x_1; if not, the d_i vanish identically and have a solution, say $(1, 1, \ldots, 1)$ and the f_i have a solution $(1, 0, \ldots, 0)$ with the coefficients of the x_1 terms 0.

Lemma 3: The system $\mathcal{F}$ has a resultant system of integral polynomials b_j in the coefficients of the f_i such that for a specialization of the coefficients of the f_i, $\mathcal{F}$ has a non-trivial common solution iff the $b_j = 0$; further, the b_j are homogeneous in the coefficients of the forms.

Elimination procedure: Successively eliminate $x_1, x_2, \ldots, x_n$. At each step, the d_i obtained by eliminating previous x_i are forms, we can continue the elimination procedure until only x_n remains and the resultant system becomes: ${x_n}^{s_1} b_1, {x_n}^{s_2} b_2, \ldots, {x_n}^{s_k} b_k$ and by the above ${x_n}^{s_j} b_j = 0 \,(\mathrm{mod}\ (f_1, \ldots, f_n))$. If elimination results in a non-zero constant, there is no common solution and we get $1 = 0 \,(\mathrm{mod}\ (f_1, f_2, \ldots, f_r))$.

Observe that not all solutions can be obtained by specialization. Consider $f_1 = x_1^2 + x_1 x_2$, $f_2 = x_1 x_2 + x_2^2 + x_1 + x_2$, $(x_1 + x_2)$ is a common factor so the resultant vanishes. $\xi_1 = -\xi_2$ is a solution; however, if $\xi_2 = -1, \xi_1 = 0$ is also solution which does not fit the specialization solution.

For the next few paragraphs, the system $\mathcal{F}$ consists of r forms, $f_1, ..., f_r$ in n variables with indeterminant coefficients. The indeterminants in f_1 are $a_1, \ldots, a_\omega$, the indeterminants in f_2 are $b_1, \ldots, b_\omega$ and the indeterminants in f_r are $e_1, \ldots, e_\omega$. When $r = n$ the resultant system is generated by a single polynomial, R, called the resultant.

Let $\mathcal{F}$ be a system of forms as above with $deg(f_i) = l_1$ and $l_1 = \alpha, l_2 = \beta, \ldots, l_r = \epsilon$. By the above, $\exists T \in \mathbb{Z}[a_1, \ldots, e_\omega]$ such that ${x_i}^\tau T = 0 \,(\mathrm{mod}\ (f_1, \ldots, f_n))$. T is called an inertial form. Set $f_1 = f_1^* + a_\omega {x_n}^\alpha$, $f_2 = f_2^* + b_\omega {x_n}^\beta$, ... , $f_n = f_n^* + e_\omega {x_n}^\epsilon$, substituting $a_\omega = -\frac{f_1^*}{x_n^\alpha}$, ..., $e_\omega = -\frac{f_r^*}{x_n^\alpha}$, we get $T(a_1, \ldots, -\frac{f_1^*}{x_n^\alpha}, \ldots, -\frac{f_r^*}{x_n^\alpha}) = 0$ (Condition "A") and this actually holds for all i if it holds for any x_i. Conversely, if Condition "A" is satisfied, ${x_n}^\tau T = 0 \,(\mathrm{mod}\ (f_1, \ldots, f_r))$.

Proof: We can use Condition A to rearrange T in powers of $a_\omega + \frac{f_1^*}{x_n^\alpha}, \ldots, e_\omega + \frac{f_r^*}{x_n^\epsilon}$ and the term independent of the powers vanishes so $T = 0 \,(\mathrm{mod}\ (a_\omega + \frac{f_1^*}{x_n^\alpha}, \ldots, e_\omega + \frac{f_r^*}{x_n^\epsilon}))$; multiplying through by the largest power of x_n in the denominators, we get $x_n^\tau T = 0 \,(\mathrm{mod}\ (f_1, f_2, \ldots, f_r))$. The inertial forms form and ideal $\mathcal{I}$ which is prime and a basis for $\mathcal{I}$ thus forms a resultant system.

Theorem: If the number of forms, f_i, is less than the number of variables, n, then there is no inertial form distinct from 0; if $r = n$, there is no inertial form independent of e_ω and distinct from 0.

The proof uses the following *Lemma:* When a sequence of polynomials $f_1, \ldots, f_s$ in indeterminants $a_1, a_2, \ldots, a_p, x_1, x_2, \ldots, x_q$ is algebraically dependent in $k[a_1, \ldots, a_p]$, this dependence is valid for every specialization $a_p = \alpha$.

Proof of Lemma: Since $F(a_1, \ldots, a_p, f_1, \ldots, f_s) = 0$ and $F(a_1, \ldots, a_p, z_1, \ldots, z_s) \neq 0$, $F(a, z)$ is not divisible by $(a_p - \alpha)$ or we could reduce the relations. So $F(a_1, \ldots, a_{p-1}, \alpha, f_1, \ldots, f_s) \neq 0$.

Proof of theorem: If $r < n$, by Condition "A", $-\frac{f_1^*}{x_n^\alpha}, \ldots, -\frac{f_r^*}{x_n^\alpha}$ would be algebraically dependent relative to $k[a_1, \ldots, a_{\omega-1}, e_1, \ldots, e_{\omega-1}]$ and this continues to be true if $x_n = 1$. If $r = n$

and the hypothesis is false, $-\frac{f_1^*}{x_n^\alpha}, \ldots, -\frac{f_{n-1}^*}{x_n^\delta}$ would be algebraically dependent relative and we can set $x_n = 1$. In both cases, the lemma applies and we can specialize over any of the indeterminants without losing dependency. Choose a specialization so $f_1, \ldots, f_s^\delta \to x_1^\alpha, \ldots, x_s^\delta$. This is a contradiction since these terms are algebraically independent.

Theorem: If $r = n$, there is a non-vanishing inertial form D_e, homogeneous in the indeterminants and of degree $L_n = l_1 l_2 \ldots l_{n-1}$ in the e_j.

Proof: Put $l = 1 + \sum_i^n (l_i - 1)$ and consider, $\mathcal{P}$, the monomials of degree l in the x_i. $\mathcal{P}$ is a disjoint union of the following sets: monomials of degree l containing ${x_1}^{l_1}$, monomials of degree l containing ${x_2}^{l_2}$ but not ${x_1}^{l_1}$, ..., monomials of degree l containing ${x_n}^{l_n}$ but not ${x_1}^{l_1}$, ${x_2}^{l_2}$, etc. Suppose $H_{l-l_1}^{(m)}$ are the complementary monomials of the elements of the disjoint sets, i.e. - ${x_1}^{l_1} H_{l-l_1}^{(m)}$ are in the disjoint sets. $H_{l-l_n}^{(m)}$ has $l_1 l_2 \ldots l_{n-1}$ power products ($x_1^k, 0 \le k < l_1$, etc). Now form $H_{l-l_i}^{(m)} f_i$. Since there are as many of these as power products, the matrix is square. Denote its determinant as D_e which has the value 1 under the specialization $f_i = {x_i}^{l_i}$. Multiplying the equations $H_{l-l_i}^{(j)} f_i = \sum a_{mk} H_l^{(k)}$ by the subdeterminants of a column of D_e and adding, the left hand side becomes linear in the f_i and the right hand side, $D_e H_l^{(k)}$. Letting $H_l^{(k)} = x_i^l$, we get $D_r x_i^l = 0 \,(\mathrm{mod}\, (f_1, f_2, \ldots, f_r))$ and D_e is homogeneous in each form, f_i and has degree L_n in the coefficients of f_n.

Now, let $f_1, f_2, \ldots, f_n$ be forms in $x_1, x_2, \ldots, x_n$ with indeterminate coefficients and $\mathcal{I}$ the ideal generated by the inertial forms. **Theorem:** If R is a polynomial of minimal degree in e_ω, every element of $\mathcal{I}$ is divisible by R. R is the resultant.

Proof: Arrange R in powers of $e_\omega, R = S{e_\omega}^\lambda + \ldots$. If T is in $\mathcal{I}$, we can get a polynomial, $T' = S^j T - QR$ of lower degree which is also in $\mathcal{I}$ but then $T' = 0$ and $R \mid T$. Note if R vanishes for a specialization, every element of $\mathcal{I}$ does also and the f_i have a common 0; conversely, if the f_i have a common zero, since ${x_i}^\tau R = A_1 f_1 + \ldots + A_n f_n$, substitution makes the right side of the equation 0 but at least one $x_i \neq 0$ so $R = 0$. We have: **Theorem**: $R(gh, f_2, \ldots, f_n) = R(g, f_2, \ldots, f_n) R(h, f_2, \ldots, f_n)$, R is homogeneous of degree L_1 in the coefficients of F_1, homogeneous of degree L_2 in the coefficients of F_2, ..., and homogeneous of degree L_n in the coefficients of F_n, $R = (D_a, D_b, \ldots, D_e)$ is a principal ideal and the resultant contains a principal term ${a_1}^{L_1} \ldots {e_\omega}^{L_n}$.

Bezout's theorem: If $n - 1$ homogeneous equations have a finite number of solutions then sum of the multiplicities equals the product of the degrees of the equations.

Proof of Bezout: Suppose the system $\mathcal{F}, r = n$ has a finite number of non-trivial solutions $(\xi_1^{(\alpha)}, \ldots, \xi_n^{(\alpha)})$, $\alpha = 1, 2, \ldots, q$. Add the form $l = u_1 x_1 + \ldots + u_n x_n$ and form the resultant system $b_1(u), b_2(u), \ldots, b_t(u)$. The resultant system has a solution iff $l_\alpha = u_1 {\xi_1}^{(\alpha)} + \ldots + u_n {\xi_n}^{(\alpha)} = 0$. By the Nullstellensatz: $(b_i(u))^{\tau_i} = 0 \,(\mathrm{mod}\, (\prod_\alpha l_\alpha))$ and $(\prod_\alpha l_\alpha)^\tau = 0 \,(\mathrm{mod}\, D(u))$ where $D(u) = (b_1(u), \ldots, b_t(u))$. So $D(u) = \prod_\alpha {l_\alpha}^{\rho_\alpha}$ (the ρ_α's are the multiplicities). If we consider $n-1$ forms f_i and add the form $l = u_1 x_1 + \ldots + u_n x_n$, we get Bezout's theorem.

Berlekamp polynomial factorization over F_q: $f(x)$ square free so $f(x) = p_1(x) \ldots p_r(x)$. Note that $v(x)^p = v(x)$ and $(v(x) - 0)(v(x) - 1) \ldots (v(x) - (p-1)) \,(\mathrm{mod}\, f(x))$ and $\exists s_i \in F_q : (f(x), v(x) - s_i) = p_i(x)$. Compute $x^{iq} \,(\mathrm{mod}\, f(x)) = \sum q_{ij} x^j$. Find null space of $Q - I$ with basis $v_1(x), \ldots, v_r(x)$. Compute $(f(x), v_k(x) - \alpha), \alpha \in F_q$. $f_n(x) = \frac{(x^n - 1)}{\prod_{d|n, d<n} f_d(x)}$. For *distinct factors*, note that if $q(x)$ is irreducible of degree d then $q(x) \mid x^{p^d} - x$ but $q(x) \mid x^{p^c} - x, c < d$. To use this, rull out square free again, set $w(x) = x$,

$d = 0$ and repeatedly check $g_d(x) = w(x) - x, v(x)$ and replace d by $d+1$, $w(x)$ by $w(x)^p$, and $v(x)$ by $\frac{v(x)}{g_d(x)}$.

Submodules of finitely generated free modules over a PID: Let D be a PID and $D^{(n)}$ be a free module of rank n over D. Then any submodule, K of $D^{(n)}$ is free with base $m \leq n$ elements.

Proof: By induction. For $n = 1$, K is isomorphic to a principal ideal. Suppose the result is true for $n-1$. Let $x_1, \ldots, x_n$ be a free basis for M. If K is contained in any module generated by all but one of the x_i, were done by induction. Let π_i be the projection on the i-th basis element. $im((\pi_i)_{|K})$ is a principal ideal generated by p_i. WLOG let $p = p_1$ generate the maximal ideal among these, so $p|p_i, \forall i$. $\exists k \in K : k = px_1 + pd_2x_2 + \ldots + pd_nx_n$. Put $y = x_1 + d_2x_2 + \ldots + d_nx_n$. $M = Dy \oplus Dx_2 \oplus \ldots \oplus Dx_n$ and $py \in K$. Set $K_1 = (K \cap \langle x_2, \ldots, x_n \rangle)$. $K = (Dp)y + K_1$ and $Dpx_1 \cap K_1 = \{0\}$ so $K = Dpy \oplus K_1$. Since $K_1 \subseteq \langle x_2, x_3, \ldots, x_n \rangle$, the result follows now by applying the induction hypothesis.

Multivariate division algorithm: Fix a monomial order ($\leq$) for terms in $x_1, x_2, \ldots x_n$. Denote leading term of f under this order as $in_{\leq}(f)$. The division algorithm for f with respect to the monomial order produces $f(x) = a_1(x)f_1(x) + \ldots + a_m(x)f_m(x) + r(x)$ where $r = 0$ or r is a linear combination of monomials none of which are divisible by $in_{\leq}(f_i)$. This is written as $r = f^F$. *Procedure for multi-variable division algorithm:* Set $r \leftarrow f(x), a_i(x) \leftarrow 0$. Pick ordering of $f_1(x), f_2(x), \ldots, f_m(x)$. If $in_{\leq}(f_j)|in_{\leq}(r)$ for any j, pick first such j, set $t \leftarrow \frac{in_{\leq}(r)}{in_{\leq}(f_j)}$, $s \leftarrow s - tf_j(x)$, $a_j(x) \leftarrow a_j(x) + t$; repeat this step until if condition fails. $r \leftarrow s$. In general, the result depends on the ordering of the $f_j(x)$.

Grobner Basis: A finite subset $G = \{g_1, g_2, ..., g_s\}$ is a Grobner basis for an ideal I with respect to the monomial order $\leq$ if $\langle in_{\leq}(g_1), in_{\leq}(g_2), ..., in_{\leq}(g_s) \rangle = \langle in_{\leq}(I) \rangle$. Equivalently, if $f \in I$, $in_{\leq}(g_i)|in_{\leq}(f)$ for some i. If G is a Grobner basis f^G is independent of the order of the $f_i(x)$. If G is a Grobner basis and $I = \langle G \rangle$, $f \in I$ iff $f^G = 0$.

Dickson's Lemma: If $S \subseteq N^n$ then $\exists v_1, v_2, \ldots v_m$ such that $S \subseteq (v_1 + N^n) \cup (v_2 + N^n) \cup \ldots \cup (v_m + N^n)$. Consequence: Every ideal has a Grobner basis.

Proof: Let $S = \{v : x^v = in_{\leq}(f), f \in I\}$. By Dickson, $S \subseteq \bigcup_i (v_i + N^n), i = 1, 2, \ldots m$. If $f(x) \in I$, $ax^w = in_{\leq}(f), w = v_i + v$ for some i, v then $x^w = x^{v_i}x^v$ hence $in_{\leq}(f_i)|in_{\leq}(f)$.

Buchberger reduction: $f \in R$ reduces to 0 with respect to $f = \langle f_1, f_2, \ldots, f_m \rangle \subseteq R - \{0\}$ iff $\exists a_1, a_2, \ldots, a_m \in R$: $f = a_1f_1 + a_2f_2 + \ldots + a_mf_m$ and $in_{\leq}(a_if_i) \leq in_{\leq}(f)$ if $a_if_i \neq 0$. This is denoted by $f \rightarrow_F 0$. Let $G = (g_1, g_2, \ldots, g_m)$, $I = \langle G \rangle$. If $f \rightarrow_G 0$ for all $f \in I$ then G is a Grobner basis. If G is a Grobner basis for I, $f^G = 0$ iff $f \rightarrow_G 0, \forall f \in I$. $S(f, g) = \frac{x^\gamma}{in_{\leq}(f)}f - \frac{x^\gamma}{in_{\leq}(g)}g$, where $x^\gamma = LCM(in_{\leq}(f), in_{\leq}(g))$. If $S(f_i, f_j) \rightarrow_F 0, \forall i, j$ then $f \rightarrow_F 0, \forall f \in I$. F is a Grobner basis iff $S(f_i, f_j) \rightarrow_F 0, \forall i, j$ iff $S(f_i, f_j)^F = 0, \forall i, j$.

Buchberger Algorithm: Test $S(f_i, f_j)^F \neq 0$, $F = F \cup \{S(f_i, f_j)\}$. Do this until all $S(f_i, f_j)^F = 0$. This procedure terminates.

Minimal Grobner: $in_{\leq}(f_i)$ does not divide $in_{\leq}(f_j)$ and coefficients are 1. *Reduced Grobner:* Minimal Grobner where $in_{\leq}(f_i)$ does not divide any term of $in_{\leq}(f_j)$. *Example:* $F = (x^2 + y, x^2y + 1)$. $S(x^2+y, x^2y+1) = y^2-1$, (x^2+y, x^2y+1, y^2-1) is a Grobner basis. *Elimination ideals:* $I_l = I \cap k[x_{l+1}, ..., x_n]$.

More on Resultants. Condition 1: $F_0(x_0, x_1, \ldots, x_n) = F_1(x_0, x_1, \ldots, x_n) = \ldots = F_n(x_0, x_1, \ldots, x_n) = 0$, with each F_i homogeneous of degree d_i in the x_i. Let $F_i(x_0, x_1, \ldots, x_n) = \sum_{|\alpha|=d_i} u_{i,\alpha}x^\alpha$. **Theorem 1:** Fix $d_0, d_1, \ldots, d_n$, there is a unique polynomial $Res \in \mathbb{Z}[u_{i,\alpha}]$ such that if $u_{i,\alpha}$ are replaced by the

corresponding $c_{i,\alpha} \in \mathbb{C}$ and F_i is homogeneous of degree d_i then (a) the equations of condition 1 have a non-trivial solution in $\mathbb{C}$ iff $Res(F_0, F_1, \ldots, F_n) = 0$, (b) $Res(x_0^{d_0}, x_1^{d_1}, \ldots, x_n^{d_n}) = 1$, (c) Res is irreducible. Sometimes we write $Res_{d_0,d_1,\ldots,d_n}$ to emphasize degrees. Note that $Res_{1,1,\ldots,1}$ is just the determinant. **Theorem 2:** For fixed $j, 0 \leq j \leq n$, Res is homogeneous in $u_{j,\alpha}$ of degree $d_0 \cdot d_1 \cdot d_{j-1} \cdot d_{j+1} \cdot d_n$; further, $Res(F_0, \ldots, F_{j-1}, \lambda F_j, F_{j+1}, \ldots, F_n)\lambda^{d_0 \cdot d_1 \cdot d_{j-1} \cdot d_{j+1} \cdot d_n} Res(F_0, F_1, \ldots, F_n)$ and the total degree of Res is $\sum_{j=0}^{n} d_0 \cdot d_1 \cdot d_{j-1} \cdot d_{j+1} \cdot d_n$. Res is alternating in the F_i and $Res(gh, F_2, \ldots, F_n) = Res(g, F_2, \ldots, F_n)Res(h, F_2, \ldots, F_n)$. *Example:* $Res_{2,2,2}(F_0, F_1, F_2)$ has 18 variables of total degree 12 and $21,894$ terms. If $f(x) = a_l x^l + \ldots + a_0$ and $g(x) = b_m x^m + \ldots + b_0$ then $Res(f, g, x) = a_l^m b_m^l \prod_{i=1}^{l} \prod_{j=1}^{m} (\xi - \eta_i) = a_l^m \prod_{i=1}^{l} g(\xi_i) = b_m^l \prod_{i=1}^{m} f(\eta_i)$. Put $A_f = k[x]/(f(x))$ and let $[h]_f$ be the natural map from $k[x] \to A_f$, further, let $m_g : [h]_f \mapsto [gh]_f$ then m_g is a linear map and $Res(f, g, x) = det(m_g)$.

1.2.4 Linear Algebra

Homomorphisms on modules: Left module M over R with $RM \subset M$, $1m = m, (r + s)m = rm + sm$, etc. Notation: $End_R(X) = Hom_R(X, X)$. $Hom_R(U, V) = \{f, f : U \to V, f(r_1 u + r_2 v) = r_1 f(u) + r_2 f(v)\}$ where $r_i \in R$.

Definition: If V is a vector space (or module) then V^*, the set of linear functions over V, is the *dual space*.

Theorem: If V is finite dimensional, $dim(V) = dim(V^*)$. $V \approx V^{**}$. Observe that the solution space is the kernel of linear map, L. $colRank + dim(ker(L)) = n$. $rowRank + dim(ker(L)) = n$.

Proof: Let $L = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}$. $L : \mathbb{R}^n \to \mathbb{R}^m$. The image of L is the column space of L and the kernel of L is the solution space to $Lx = 0$. $\mathbb{R}^n/ker(L) \cong im(L)$ so $n - dim(ker(L)) = colRank(L)$. Now, $ker(L)$ is the space of vectors in $\mathbb{R}^n$ orthogonal to the rows of L so $dim(ker(L)) + rowRank(L) = n$. So, $rowRank(L) = colRank(L)$.

Theorem: Suppose $r_1, r_2, \ldots, r_m \in \mathbb{R}^n$ are linearly independent and $S = \{x \in \mathbb{R}^n : x \cdot r_i = 0\}$ then $dim(S) = n - m$.

Proof: Put $W = \{r_1, r_2, \ldots, r_m\}$. $r_i \notin S$ since $r_i \cdot r_i \neq 0$ so $dim(S) \leq n - m$. Define $\alpha : x \mapsto (x \cdot r_1, \ldots, x \cdot r_m)$. Then $dim(ker(\alpha)) = dim(S)$ and $dim(ker(\alpha)) + dim(im(\alpha)) = n$. Since $dim(im(\alpha)) \leq m$, $dim(S) + m \geq n$ so $dim(S) \geq n - m$.

Theorem: The row rank, r, equals column rank, c.

Proof: Let $A = (a_{ij})$ be an $m \times n$ matrix. Let $\langle S_1, \ldots, S_r \rangle$ be a basis for the row space. Put $S_i = (s_{ij}), 1 \leq j \leq n, 1 \leq i \leq r$. Let row i, $R_i = (a_{i1}, a_{i2}, \ldots, a_{in})$. $R_i = \sum_{t=1}^{r} k_{it} S_t$. So $a_{ij} = \sum_{t=1}^{r} k_{it} s_{tj}, 1 \leq j \leq n, 1 \leq i \leq m$ and the column vectors $(k_{1i}, k_{2i}, \ldots, k_{mi})^T, 1 \leq i \leq r$ span the column space. Thus $c \leq r$. The same holds for A^T and so $r \leq c$ and $r = c$.

Artin's proof:
Lemma: If $W \subset V$ are vector spaces over k and $W^\perp \subset V^*$ then $dim(W) + dim(W^\perp) = dim(V)$.
Proof of result: Let $T : k^n \to k^m$ be the linear transformation represented by the matrix M with rows $r_1, r_2, \ldots, r_m$ and columns $c_1, \ldots, c_n$ and let the row space of M be R and the column space, C; finally, let $r = dim(R)$, $c = dim(C)$ and $W = ker(T)$. Since $dim(Im(T)) + dim(W) = n = dim(V)$, $r = n - dim(W)$ and $dim(W) + dim(W^\perp) = n$, it suffices to show $dim(W^\perp) = r$.

Note that $r_i \cdot w = 0$ for $w \in W$ so, if λ_i is the usual dual basis of V^* with respect to $\langle e_1, e_2, \ldots, e_n\rangle$ where $\langle e_1, e_2, \ldots, e_k\rangle = W$. Let λ_j be the natural dual basis and note that $R \subseteq \langle e_{k+1}, e_{k+2}, \ldots, e_n\rangle$ since $r_i \cdot \lambda_j = 0$ for $j \leq k$. Now let $b_{k+1}\lambda_{k+1} + \ldots + b_n\lambda_n = \lambda \in W^\perp$. Consider $\varphi : \lambda \mapsto b_{k+1}e_{k+1} + \ldots + b_ne_n$. If $\varphi(\lambda) = 0$, $\lambda = 0$ so $dim(R) = dim(W^\perp)$ and the result holds.

Here's still another proof.

Theorem: If $A : V \to W$ is a linear transformation (i.e, $A \in Hom_{\mathbb{R}}(V, W)$) between two finite dimensional vector spaces over $\mathbb{R}$, then $V = U \oplus S$ where $U \cong im(A)$ and $S = ker(A)$.

Proof: Let $\langle u_1, u_2, \ldots, u_k\rangle$ be a basis for $im(A)$, so $k = dim(im(A))$. Pick $v_1, \ldots, v_k \in V$: $A(v_i) = u_i, 1 \leq i \leq k$. First observe $\langle v_1, \ldots, v_k\rangle$ are linearly independent because $a_1v_1 + \ldots + a_kv_k = 0$ implies $a_1A(v_1) + \ldots + a_kA(v_k) = 0$ so $a_1u_1 + \ldots + a_ku_k = 0$ and all the a_i are 0 since $\langle u_1, u_2, \ldots, u_k\rangle$ is a basis; also note that $U = span(v_1, \ldots, v_k) \cong im(A)$. Let $S = ker(A)$. $V = U + S$ so we need only show $U \cap S = 0$. If $v = a_1v_1 + \ldots + a_kv_k \in S$ then $a_1A(v_1) + \ldots + a_kA(v_k) = 0$ but since $\langle u_1, u_2, \ldots, u_k\rangle$ is a basis, we must have $v = 0$.

Theorem: Let $V = \mathbb{R}^n$ and $\langle v_1, \ldots, v_m\rangle$ be a set of linearly independent vectors in V. Put $S = \{v \in V : (v_i, v) = 0, i = 1, \ldots, m\}$. Finally, put $s = dim(S)$. $s + m = n$.

Proof: Put $W = span(v_1, \ldots, v_m)$. First note that $S \cap W = 0$ because $v \in S \to (v, w) = 0, \forall w \in W$. If $v \in W$, this means $(v, v) = 0$ so $v = 0$. Now, $dim(W + S) = dim(W) + dim(S) - dim(S \cap W) = dim(W) + dim(S) \leq n$ so $n - m \geq s$. Define $\alpha : V \to \mathbb{R}^m$ by $\alpha(v) = ((v_1, v), (v_2, v), \ldots, (v_m, v))$. $\alpha \in Hom_{\mathbb{R}}(\mathbb{R}^n, \mathbb{R}^m)$ so $im(\alpha) + ker(\alpha) = \mathbb{R}^n$. $ker(\alpha) = S$ and $dim(im(\alpha)) \leq m$ since $im(\alpha) \subseteq \mathbb{R}^m$. Thus $m + s \geq n$ and $s \geq n - m$, this, along with the previous inequality gives $n - m = s$.

Theorem: Let $A = \begin{pmatrix} a_{11} & a_{12} & ... & a_{1n} \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mn} \end{pmatrix}$. $A : \mathbb{R}^n \to \mathbb{R}^m$. Let r be the row rank of A and c be the column rank. Then $r = c$.

Proof: Put $a_i^R = (a_{i1}, a_{i2}, \ldots a_{in}), 1 \leq i \leq m$ and $a_j^C = (a_{1j}, a_{2j}, \ldots a_{mj})^T, 1 \leq j \leq n$. Put $S = \{x \in \mathbb{R}^n : (a_i^R, x) = 0, 1 \leq i \leq m\}$ and $s = dim(S)$. Note that $S = ker(A)$. By the previous theorem, $n = s + r$. The column space of A is $V_{CS} = span(a_1^C, \ldots, a_n^C)$ which is just $im(A)$. So $n = c + s$. Thus $r = c$.

Change of basis for matrix: Let $[e] = \{e_1, \ldots, e_n\}$ be a basis for V_n and let L be a linear transformation on V_n. Let $v_{[e]} = [c_1, c_2, ..., c_n]^T$ denote the coordinates of v with respect to $[e]$: $v_{[e]} = c_1e_1 + ... + c_ne_n$. Let $L_{[e]}$ denote the matrix for L with respect to $[e]$: $L_{[e]} : e_i \mapsto \sum_j a_{ji}e_j$. Then $L_{[e]}v_{[e]} = (Lv)_{[e]}$. If $f_i = \sum_j b_{ji}e_j$ is another basis, $P = (b_{ij})$ is called the transition matrix from $[f]$ to $[e]$ (equivalently, $P[e_1, e_2, \ldots, e_n] = [f_1, f_2, \ldots, f_n]$) and P^{-1} is the transition matrix from $[e]$ to $[f]$ (note the sum over the first index). $Pv_{[f]} = v_{[e]}$ and $v_{[f]} = P^{-1}v_{[e]}$. Finally, $L_{[f]} = P^{-1}L_{[e]}P$. The same holds over free modules. Alternate notation: $L : V \to W$, V has basis $\mathcal{B}$ and W has basis $\mathcal{B}'$ with $L(w_i) = \sum_j a_{ij}v_j$ then $M_{\mathcal{B}'}^{\mathcal{B}}(F) = A^T$. If $\mathcal{B}$ and $\mathcal{B}'$ are over the same space, $M_{\mathcal{B}'}^{\mathcal{B}'}(F) = N^{-1}M_{\mathcal{B}}^{\mathcal{B}}(F)N$ where $N = M_{\mathcal{B}}^{\mathcal{B}'}(id)$.

Theorem: The group of *affine transformations* is isomorphic to the subgroup of the matrices with last column $(0, 0, \ldots, 0, 1)$. The translations form a normal subgroup.

Cayley-Hamilton Theorem: Any matrix, A, acting on a vector space V of dimension n, over a field, F, whose characteristic roots lie in F (For example, if F is algebraically closed field) is similar to a triangular one. The minimum polynomial divides the characteristic polynomial.

Proof: The second statement follows from the first since the characteristic roots, λ_i appear on the diagonal of the triangular matrix and the characterisitic polynomial is thus $f(x) = \prod_{i=1}^{n}(x - \lambda_i)$. $f(A) = 0$ so the minimal polynomial divides the characteristic polynomial. The proof of the first statement is by induction on n. It is true for $n = 1$. Suppose it's true for $n - 1$. A has an eigenvalue, say, λ_1 in F with $Av = \lambda_1 v_1, v_1 \neq 0$. Put $W = \{av_1, a \in F\}$. A acts on V/W which has dimension $< n$ so by induction, $\exists v_2, \ldots, v_n$ and $a_{ij} \in F$: $A\overline{v}_2 = a_{22}\overline{v}_2$, $A\overline{v}_3 = a_{32}\overline{v}_2 + a_{33}\overline{v}_3$, and so on. Let $v_i, i > 1$ be corresponding elements of V. $Av_2 - a_{22}v_2 \in W$ and so on. Thus A is triangular in the basis $\{v_1, \ldots, v_n\}$.

Definitions: Let A^* denote the *adjoint* (conjugate transpose). $(Ax, y) = (x, A^*y)$. A *hermitian matrix* is self adjoint over complex numbers. A *symmetric matrix* is self adjoint over reals. A *unitary matrix* $AA^* = I$; equivalently: A is length preserving: $(Ax, Ay) = (x, y)$. A is *nilpotent* if $\exists q$: $A^q = 0$, smallest q is degree of nilpotence. A is *normal* if $AA^* = A^*A$.

Theorem: If T is any linear transform on V_n, $\exists M_0, M_1, \ldots, M_n$: (i) $AM_k \subseteq M_k$, (ii) $dim(M_j) = j$, (iii) $\{0\} = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_n = V_n$.

Proof:

Theorem: If A is a linear transform on V_n with proper values $\lambda_1, \lambda_2, \ldots, \lambda_p$ having multiplicity $m_1, m_2, \ldots, m_p$ then $V_n = M_1 \oplus \ldots \oplus M_p$ with $AM_j \subseteq M_j$, $dim(M_j) = m_j$ and $A - \lambda_j I$ is nilpotent on M_j.

Proof:

Theorem: If A is nilpotent of degree q, $\exists x$: $A^{q-1}x \neq 0$ and $x, Ax, A^2x, \ldots A^{q-1}x$ are linearly independent. Every linear transform is the direct sum of a nilpotent and an invertible transform.

Proof: The existence of x is guarenteed by nilpotence. If $a_0x + a_1Ax + a_2A^2x + \ldots a_{q-1}A^{q-1}x = 0$, applying A $q - 1$ times, we get $a_0A^{q-1}(x) = 0$ which is a contradiction.

Theorem: If A is symmetric and X is orthogonal then XAX^{-1} is symmetric.

Proof: Since X is orthogonal, $X^{-1} = X^T$. $XAX^{-1} = (XAX^T)^T = XA^TX^T = XAX^T = (XAX^{-1})^T$.

Theorem: T is orthogonal (unitary) iff it takes orthonormal basis into orthonormal basis which happens iff $TT^* = I$.

Proof: If T is unitary and $\langle v_1, \ldots, v_n \rangle$ is an orthonormal basis, $(Tv_i, Tv_j) = (v_i, v_j) = \delta_{ij}$ and $\langle Tv_1, \ldots, Tv_n \rangle$ is an orthonormal basis. If $Tv_i = w_i$ and $\langle v_1, \ldots, v_n \rangle$ and $\langle w_1, \ldots, w_n \rangle$ are both orthogonal basis extending linearly we get, $(Tx, Ty) = (x, y)$ and T is unitary.

Theorem: (a) If $S^*S(v) = 0$, $S(v) = 0$. Suppose N is *normal*. (b) $N(v) = 0 \rightarrow N^*(v) = 0$. (c) If $N(v) = \lambda v$, $N^*(v) = \overline{\lambda}v$. (d) If $N^k(v) = 0$ then $N(v) = 0$. (e) If $N(v) = \lambda v, N(w) = \mu w, \lambda \neq \mu$ then $(v, w) = 0$.

Proof: For (a), $(S^*S(v), v) = 0 = (S(v), S(v))$ and so $S(v) = 0$. For (b), $(N^*(v), N^*(v)) = (NN^*v, v) = (N^*Nv, v) = (Nv, Nv) = 0$. For (c), $(N - \lambda)(N^* - \overline{\lambda})$. Since $(N - \lambda)$ is normal and $(N - \lambda)(v) = 0$, (b) gives $(N - \lambda)^*(v) = 0$ and the result follows. For (d), let $S = N^*N$ then $S^kv = (N^*)^kN^kv = 0$. Since $S^* = S$, $S(v) = 0$ by (a) and again by (a) $N(v) = 0$. For (e), $\lambda(v, w) = (Nv, w) = (v, N^*w) = (v, \overline{\mu}w) = \mu(v, w)$ and the result follows.

Spectral Theorem: If T is *normal* ($TT^* = T^*T$), $\exists E_1, \ldots, E_r$ such that $T = \sum_i^r \lambda_i E_i$ with $T = \sum_i^r E_i = I$, $E_i E_j = 0$ and transforming matrix, A, unitary ($\overline{A}^t = A^{-1}$).

Proof: Let $\lambda_1, \ldots, \lambda_k$ be the distinct characteristic roots of T. By the primary decomposition theorem, $V = V_1 \oplus \ldots \oplus V_n$ and each V_i is annihilated by $(T - \lambda_i)^{n_i}$. Vectors in different V_i's are orthogonal and each V_i has an orthonormal basis by Gram-Schmidt. T can be transformed into an upper triangular matrix with its eigenvalued on the diagonal, sinfe T is normal, this matrix must be diagonal.

Theorem: If A is symmetric there is a P such that $P^T AP$ is diagonal. All the eigenvalues are real.

Proof: Diagonalizability follows from the Spectral theorem. If $Av = \lambda v$, $(AA^T v, v) = (Av, Av) = \lambda^2 > 0$ so the eigenvalues are real.

Sylvester's Theorem: Every real quadratic form is equivalent to a diagonal one with a signature of positive and negative coefficients. Two forms are equivalent iff they have the same rank and signature.

Proof: Since the matrix for the form is real and symmetric it can be brought into diagonal form by an orthogonal transformation and the eigenvalues are the diagonal elements of the matrix. The rank is invariant and so the number of nonzero elements is an invariant. Because there are square roots, we can assume the elements are ± 1. If r is the number of -1's and s is the number of 1's we need only show these are invariants. Since the subspace of vectors on which the form is positive is an invariant, we're done.

Definition: Extreme point in convex set: P with no Q_1, Q_2 such that $P = tQ_1 + (1-t)Q_2$, $t > 0$.

Krien Millman Theorem: If S is a closed, bounded convex set, then S is the convex closure of its extreme points.

Principal Axis Theorem: Any real quadratic form is equivalent to one with $Q(\eta) = \lambda_1 {x_1}^2 + \ldots + \lambda_n {x_n}^2$ with $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$.

Proof: Find eigenvector v, $V = \langle v \rangle \oplus \langle v \rangle^\perp$.

SVD: $A = U\Sigma V^T$, Σ diagonal and $UU^T = VV^T = 1$.

Theorem: An $n \times n$ matrix is *diagonalizable* iff it has n linearly independent eigenvectors. A matrix is diagonalizable iff its minimal polynomial is a product of different linear factors. Two matrices are simultaneously diagonalizable iff they are diagonalizable and commute.

Proof: The first and second statements are easy. The third statement is proved by induction on n. It is clear for $n = 1$. Let $\lambda_1, \lambda_2, \ldots, \lambda_k$ be the characteristic values of T and W_i be the null space of $T - \lambda_i$. Each W_i is an invariant space and the $T_{|W_i}$ is diagonalizeable. Since $dim(W_i) < dim(V)$ the commuting operators restricted to these spaces can be simultaneously diagonalized. Composing the diagonal bases of the restricted transformations yields a basis in which all the matricies are diagonal.

Theorem: Let $f : A \to A'$ be surjective. A, A' abelian, A' free. $\exists C \subseteq A$ such that $A = ker(f) \oplus C$.

Proof: Let $\langle x_i' \rangle$ be a basis of A' and for each $i \in I$, let $x_i \in A$ be such that $f(x_i) = x_i'$. Put $C = \langle x_i \rangle$ and $B = ker(f)$. If we have $\sum_{i \in I} n_i x_i = 0$, applying f yields $\sum_{i \in I} n_i x_i' = 0$ and $\langle x_i \rangle$ is a basis. Similarly, if $z \in C$ and $f(z) = 0$ then $z = 0$. Hence $B \cap C = 0$. Let $x \in A$. Since $f(x) \in A'$, $\exists n_i, i \in I : f(x) = \sum_{i \in I} n_i x_i'$. Applying f to $x - \sum_{i \in I} n_i x_i = b \in B$. $x \in B + C$ and so $A = B \oplus C$.

Submodules of free modules over PIDs: Let $D^{(n)}$ be a free D-module, D, a PID, with basis $X = [e_1, e_2, \ldots, e_n]^T$. If P is invertible, $Y = [e'_1, \ldots, e'_n]^T = PX$ is another basis for $D^{(n)}$. Let K be a submodule generated by $U = [u_1, \ldots, u_m]^T = AX$. A is called a relations matrix. Suppose Q is invertible so that $V = QU$ is another set of generators for K. $V = QU = QAX = QAP^{-1}Y$. $B = QAP^{-1}$ is the new relations matrix for the basis Y. A and B are called *equivalent*. In the foregoing, M is finitely generated and we note that the map $f : e_i \mapsto u_i$ extends to a homomorphism and $M \cong D^{(n)}/K$ where $K = ker(f)$. K is a submodule of $D^{(n)}$ and by a previous result, is free with a base of size $m \leq n$.

Theorem: If A is an $m \times n$ matrix with entries from a PID, D, then A is equivalent to a matrix of the form $diag(d_1, d_2, \ldots, d_r, 0, 0, \ldots, 0)$ with $d_i \neq 0$ and $d_i \mid d_{i+1}$. The proof simply requires applying elementary row and column operations to A as is done below. There, let $O_{ij} = (\delta_{il}\delta_{jk})_{1 \leq l \leq n, 1 \leq k \leq n}$ and $E_{ij}(\alpha) = I + \alpha O_{ij}$. $E_{ij}(\alpha)A$ acts on A by adding α times row j to row i. $AE_{ij}(\alpha)A$ acts on A by adding α times column i to column j.

Example: Suppose $D = \mathbb{Z}$ and $F = \mathbb{Z}^{(3)}$ is a free abelian group with basis x_1, x_2, x_3 and K is the submodule generated by $u_1 = 2x_1 + 2x_2 + 8x_3$ and $u_2 = -2x_1 + 2x_2 + 4x_3$ and $F/K = \langle x_1, x_2, x_3 | 2x_1 + 2x_2 + 8x_3 = 0, -2x_1 + 2x_2 + 4x_3 = 0 \rangle$. We have $\begin{pmatrix} 2 & 2 & 8 \\ -2 & 2 & 4 \end{pmatrix} \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \end{pmatrix}$ and $F/K = \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}$.

Structure theorem for finitely generated modules over principal ideal domains: If $M \neq 0$ is a finitely generated module over a PID, D. Then $M = Dz_1 \oplus Dz_2 \oplus \ldots \oplus Dz_s$ with $ann(z_1) \supseteq ann(z_2) \supseteq \ldots \supseteq ann(z_s)$, $z_k \neq 0$. Note $Dz_i \cong D/ann(z_i)$.

> *Proof:* First, $Dx \cong D/ann(x)$, always. Let the base of $D^{(n)}$ be $e_1, e_2, \ldots, e_n$ and let $\eta : D^{(n)} \to M$ be the canonical map $\sum_i a_i e_i \mapsto \sum_i a_i x_i$ where $\langle x_i \rangle$ are generators for M. $M \cong D^{(n)}/K$. $K = ker(\eta)$ is generated by $f_i = \sum_j a_{ij} e_j, i = 1, 2, \ldots, n$. The Smith reduced canonical relations matrix is $QAP^{-1} = diag(d_1, d_2, ..., d_r, 0, \ldots, 0)$ and $d_i \mid d_{i+1}$, $P = (p_{ij}), Q = (q_{ij})$. So $f'_i = d_i e'_i$ where $e'_i = \sum_j p_{ij} e_j$ and $f'_i = \sum_j q_{ij} f_j$. $y_i = \sum_j p_{ij} x_j$ is another set of generators for M (i.e., $M = \sum Dy_i$). If $\sum_i b_i y_i = 0$ then $\sum_i b_i e'_i \in K$ so $\sum_i b_i e'_i = \sum_i c_i f'_i = \sum_i c_i d_i e'_i$ and so $b_i = c_i d_i$ and $b_i y_i = 0, \forall i$, since each $d_i y_i = 0$, already. $ann(y_i) = (d_i)$ by construction. If d_i is a unit, $d_i y_i = 0 \to y_i = 0$ and we can drop y_i from the list of generators. Thus if the first t d_i are units, putting $z_1 = y_{t+1}, \ldots, z_s = y_n$, $s = n - t$, we get the desired result.

Notation: Let T be and endomorphism of the D-module, M $\alpha \in M$. $Z(\alpha, T)$ is the cyclic subspace generated by T. The T-annihilator of α is $(p(x))$ since D is a PID where $p(x) = x^k + c_{k-1}x^{k-1} + \ldots + c_0$. The companion matrix (matrices operating on the left) is $C_T = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 1 \\ -c_0 & -c_1 & -c_2 & \ldots & -c_{k-2} & -c_{k-1} \end{pmatrix}$.
For a vector space of V over F, $T : V \to V$, the *rational decomposition* is $V = Z(\alpha_1, T) \oplus \ldots \oplus Z(\alpha_r, T)$. Again, the PID is $D = F[x]$.

Application to a linear transformation: Suppose $e_1, \ldots, e_n$ is a basis for V over F and put $D = F[\lambda]$. Let $T(e_i) = \sum_j a_{ij} e_j$. For $g(\lambda) \in D$, $g(T)$ acts on vectors in the usual way. As above, $M \cong D^{(n)}/K$ and K has a free base over D with $m \leq n$ elements.

Lemma: $f_i = \lambda e_i - \sum_j a_{ij} e_j$ is a base for K over D.

> *Proof:* Since $Te_i = \sum_j a_{ij} e_j$, $\lambda e_i = f_i + \sum_j a_{ij} e_j$, and we can write any $g_i(\lambda) e_i$ as $\sum_i g_i(\lambda) e_i =$

$\sum_i h_i(\lambda)f_i + \sum b_i e_i$, $b_i \in F$. If this is in K, then $\sum_i b_i e_i \in K$ so $\sum_i b_i e_i = 0$. Since the e_i form a base for V over F, $b_i = 0, \forall i$ and the element K has the form $\sum_i h_i(\lambda)f_i = 0$. Suppose there is a non trivial relation between the $h_i(\lambda)$, then $\sum_{i=1}^n h_i(\lambda)\lambda e_i = \sum_{i,j=1}^n h_i(\lambda)a_{ij}\lambda e_i$ and since the e_i is a base, $h_i(\lambda)\lambda = \sum_{j=1}^n h_j(\lambda)a_{ji}$. If any $h_i(\lambda) \neq 0$ let $h_r(\lambda)$ be one of maximal degree. Clearly, $h_r(\lambda)\lambda = \sum_j h_j(\lambda)a_{jr}$ is impossible. This proves every $h_i(\lambda) = 0$ and so the f_i form a base for K.

After diagonalization, $Q(\lambda I - A)P = diag(1, \ldots, 1, d_1(\lambda), \ldots, d_s(\lambda))$. As in the proof of the structure theorem, K is generated by $f_i' = d_i e_i'$. If $P^{-1} = (p_{ij}^*)$, $v_i = \sum_j p_{ij}^* u_j$, $z_i = v_{n-s+i}$ and $V = Dz_1 \oplus \ldots \oplus Dz_s$.

Example: Suppose $Tu_1 = -u_1 - 2u_2 + 6u_3$, $Tu_2 = -u_1 + 3u_3$, $Tu_3 = -u_1 - u_2 + 4u_3$. The matrix for T in the basis $\langle u_1, u_2, u_3\rangle$ is A.

$$A = \begin{pmatrix} -1 & -2 & 6 \\ -1 & 0 & 3 \\ -1 & -1 & 4 \end{pmatrix}, Q = \begin{pmatrix} 0 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 2-\lambda & -3 \end{pmatrix}, P = \begin{pmatrix} 1 & 3 & \lambda - 3 \\ 0 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}$$

$$Q(\lambda I - A)P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & (\lambda-1) & 0 \\ 0 & 0 & (\lambda-1)^2 \end{pmatrix}, P^{-1} = \begin{pmatrix} 1 & \lambda & -3 \\ 0 & -1 & 1 \\ 0 & -1 & 0 \end{pmatrix}$$

$v_1 = u_1 + \lambda u_2 - 3u_3$, $v_2 = -u_2 + u_3$, $v_3 = -u_2$. $z_1 = v_2 = -u_2 + u_3$, $z_2 = v_3 = -u_2$, $z_3 = \lambda v_3 = u_1 - 3u_3$. So, $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}_z = \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}_u$, $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}_z = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}_u$, $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}_z = \begin{pmatrix} 1 \\ 0 \\ -3 \end{pmatrix}_u$. Thus the transition matrix between the u base and the z base is $R = \begin{pmatrix} 0 & -1 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & -3 \end{pmatrix}$ and $R^{-1} = \begin{pmatrix} 3 & -3 & 1 \\ 0 & -1 & 0 \\ 1 & -1 & 0 \end{pmatrix}$. $RAR^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 2 \end{pmatrix}$, as we can verify directly by

$$\begin{pmatrix} 0 & -1 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & -3 \end{pmatrix}\begin{pmatrix} -1 & -2 & 6 \\ -1 & 0 & 3 \\ -1 & -1 & 4 \end{pmatrix}\begin{pmatrix} 0 & -1 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & -3 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 2 \end{pmatrix}.$$

Note in the example above, the matricies are applied "from the right." Conventionally, matricies are applied from the left. We can take tranposes of all the matricies in the above example to convert the example to one where the matricies are applied conventionally. Here is an analysis using the conventional notation:
Let A be a matrix and $\langle e_1, e_2, \ldots, e_n\rangle$ the underlying basis so that $Ae_1 = (a_{11}, a_{21}, \ldots a_{n1})^T$. Put $B(\lambda) = (\lambda I - A)$ and let $f_1, f_2, \ldots, f_n$ be the columns of $B(\lambda)$. Suppose D is a PID and $\langle x_1, x_2, \ldots, x_n\rangle$ be generators of the module, M over D. Let $\eta : D^{(n)} \to M$ be defined by $\eta(c_1, c_2, \ldots, c_n) = c_1x_1 + c_2x_2 + \ldots + c_nx_n$. $D^{(n)}/K = M$ where K is is generated by the columns of $B(\lambda)$, namely, $f_1, f_2, \ldots, f_n$. Put $B(\lambda)$ in Smith normal form, $PB(\lambda)Q = diag(1, 1, \ldots, 1, d_1(\lambda), \ldots, d_s(\lambda))$. $M = D/(d_1(\lambda)) \oplus \ldots \oplus D/(d_s(\lambda))$ and $d_1(\lambda) \mid d_2(\lambda) \mid \ldots \mid d_s(\lambda)$. Put $P = (p_{ij})$, $Q = (q_{ij})$ and $P^{-1} = (p_{ij}{}^*)$. Then $e_i{}' = \sum_k p_{ki}e_k$, $f_i{}' = \sum_k q_{ki}f_k$. $e_i = \sum_k p_{ki}{}^* e_k{}'$. $f_i{}' = \sum_{k,l,m} q_{li}b_{kl}p_{mk}{}^* e_m{}'$. $ann(f_i{}') = (d_i(\lambda))$. Q is invertible so $\langle f_1{}', f_2{}', \ldots, f_m{}'\rangle$ also generates K. If $y_i = \sum_j p_{ji}x_j$, $\langle y_i\rangle$ also generates M and $Dy_i = D/(d_i(\lambda))$. When computing the rational canonical form (RCF), $v_i = \sum_k p_{ki}{}^* e_k$ and $z_i = v_{n-s+i}$. The remaining z_i required to from the basis of the RCF by applying A to the existing z_i, as above. This gives $z_i = \sum_k s_{ki}e_k$. S is the transition matrix relating the original basis to the basis in which A has standard RCF. $A_{RCF} = S^{-1}AS$. When the matricies are applied "from the right," the companion matrix, for the block having minimal polynomial

$f(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_0$, has the form:

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & -c_{n-1} \\ 1 & 0 & 0 & \ldots & -c_{n-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 & -c_0 \end{pmatrix}$$

Here are two ways to do the computation with the current example: $A = \begin{pmatrix} -1 & -1 & -1 \\ -2 & 0 & -1 \\ 6 & 3 & 4 \end{pmatrix}$, $B(\lambda) = (\lambda I - A) = \begin{pmatrix} \lambda+1 & 1 & 1 \\ 1 & \lambda & -1 \\ -6 & -3 & \lambda-4 \end{pmatrix}$. $PB(\lambda)Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & (\lambda-1) & 0 \\ 0 & 0 & (\lambda-1)^2 \end{pmatrix}$, where P is the product of the elementary row operations: $[R_3 \leftarrow R_3 + R_2][R_3 \leftarrow R_3 - (\lambda-4)R_1][R_2 \leftarrow R_1 - R_1]$. One way to compute R, the matrix with $R^{-1}AR = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}$, is to compute the revised basis using the rules: (1) $R_i \leftarrow R_i + \alpha R_j$ causes a basis change of $e_j = e_j - e_i$ and $R_i \leftrightarrow R_j$ causes a basis change of $e_j \leftrightarrow e_i$. This results in $(0, e_2 - e_1, e_3)$, the first entry should be zero and an additional entry can be computed by applying A to e_3 giving $R = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ -1 & 1 & 4 \end{pmatrix}$. We can calculate $R^{-1} = \begin{pmatrix} -1 & 1 & 0 \\ 3 & 1 & 1 \\ -1 & 0 & 0 \end{pmatrix}$. We get

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix} = \begin{pmatrix} -1 & 1 & 0 \\ 3 & 1 & 1 \\ -1 & 0 & 0 \end{pmatrix} \begin{pmatrix} -1 & -1 & -1 \\ -2 & 0 & -1 \\ 6 & 3 & 4 \end{pmatrix} \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ -1 & 1 & 4 \end{pmatrix}$$

Another way, to get R, is to compute P from the elementary row operations, so $P = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ (3-\lambda) & 1 & 1 \end{pmatrix}$ and compute $P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ \lambda-4 & -1 & 1 \end{pmatrix}$. This lets us read off, from P^{-1}, $R = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -1 \\ -1 & 1 & 4 \end{pmatrix}$. Again, the last column is computed as Ae_3 and again, we compute R^{-1}.

Observation: The *Rational Canonical Form* and *Jordan Canonical Form* are the same over an algebraically closed field.

Grove's treatment: R, a pid. $f \in Hom_R(M, N)$, M free of dimension n, N, free of dimension m. $M = \langle x_1, x_2, \ldots, x_n \rangle$, $N = \langle y_1, y_2, \ldots, y_m \rangle$. $f(x_i) = \sum_{j=1}^{m} a_{ji} y_j$. $A = (a_{ij})$.

Theorem G1: R, M, N, f as above. Put $E = Im(f)$. Suppose that over the basis for M and N, f is represented as a matrix by:

$$\begin{pmatrix} U & 0 & 0 \\ 0 & D & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

where U and D are diagonal matricies $U = diag(u_1, u_2, \ldots, u_s\rangle$ with u_i a unit and $D = diag(d_1, d_2, \ldots, d_k\rangle$ with $d_i \in R$ and $d_j \mid d_{j+1}$. Then N/E is a direct sum of cyclic modules over R, $N/E = \bigoplus_{i=s+1}^{m} R\langle y_i + E\rangle$, with invariant factors $d_1, d_2, \ldots, d_s$. N/E has rank $m - s - k$ and $dim(E) = s + k$.

Proof: $f(x_i) = u_i y_i, 1 \le u \le s$, $f(x_i) = d_i y_i, s+1 \le u \le s+k$, $f(x_i) = 0, i \ge s+k+1$. Put $W_i = R\langle y_i + E\rangle$, $s+1 \le i \le m$. $N/E = \sum_i W_i$ and $W_i \cap \sum_{i \ne j} W_j = 0$ so the sum is direct. Each $y_i + E$ has order d_{i-s}.

Theorem G2: If R is a Euclidean ring (more generally, a pid), and $A = (a_{i,j}$, an $m \times n$ matrix over R. The there are matricies P, Q over R such that $PAQ = B$ with $B = \begin{pmatrix} U & 0 & 0 \\ 0 & D & 0 \\ 0 & 0 & 0 \end{pmatrix}$. The diagonal entries are unique up to associates.

Proof: This is just the HNF algorithm over R. D is the torsion submodule of $R^m/(f(R^n)$.

Application to linear equations: Consider the linear equations $\sum_{j=1}^n a_{i,j} x_j = c_i$, $i = 1, 2, \ldots, m$. Write this as $AX = C$. Suppose we have P, Q so that $PAQ = diag(r_1, \ldots, r_k, 0, \ldots 0)$. Put $X = QY$. $AX = AQY = C$ and $PAQY = PC$. This gives the solutions in terms of Y, Now transform back to X.
Example:

$$A = \begin{pmatrix} -33 & 42 & -20 \\ 21 & -27 & 13 \end{pmatrix},\ C = \begin{pmatrix} -26 \\ 16 \end{pmatrix}$$

We find P, Q as:

$$P = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix},\ Q = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 3 \end{pmatrix}$$

which gives

$$PAQ = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix},\ PC = \begin{pmatrix} -4 \\ 6 \end{pmatrix}$$

So $y_1 = -4, 3y_2 = 6, y_3 = a$, and finally,

$$\begin{pmatrix} x_1 \\ x_2 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 3 \\ 2 & 3 & 3 \end{pmatrix} \begin{pmatrix} -4 \\ 2 \\ a \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ -2 \end{pmatrix} + a \begin{pmatrix} 2 \\ 3 \\ 3 \end{pmatrix}$$

.

Theorem G3: $R = F[x]$. Suppose N is a free module of dimension n over R with basis $\langle e_1, e_2, \ldots, e_n\rangle$ and choose a basis $\langle v_1, v_2, \ldots, v_n\rangle$ so T has the representation $A = (a_{ij})$ over this basis. Let E be the module generated by columns of $A - xI$. $V_T \cong N/E$.

Proof: Define $\phi : N \to V_T$ by $\phi(e_i) = v_i$. We show $ker(\phi) = E$. Let $z_i = \sum_{j=1}^n a_{ji} e_j = x e_i$ then $E = \langle z_i\rangle$. $\phi(z_i) = \sum_{j=1}^n a_{ji} v_j - T(v_i) = 0$ so $E \subseteq ker(\phi)$. Let $W = \langle e_i + E\rangle$, $1 \le i \le n$ and $x \in R$. $x e_i + xE \in W$ so W is a submodule of N/E. Since $N = R\langle e_1, e_2, \ldots, e_n\rangle$, $W = N/E$. If $u \in N$, $u = \sum_i c_i e_i + z$, $c_i \in F, x \in E$. $\phi(u) = \sum_i c_i \phi(e_i) + \phi(z) = \sum_i c_i v_i$ and so $u \in ker(\phi)$ iff $c_i = 0$ so $u \in E$.

RCF: Let A, R, N and V be as above and $M = N = R^n$. If $z_i \in N$ is the ith column of $A - xI$, define $f : M \to N$ by $f(e_i) = z_i$ and $E = im(f) = R\langle z_1, z_2, \ldots, z_n\rangle$. By theorem G3, $V_T \cong N/E$. The matrix for f over $\langle e_i\rangle$ is $A - xI$ and by theorem G2, $\exists P, Q : PAQ = B$. $B = \begin{pmatrix} U & 0 & 0 \\ 0 & D & 0 \\ 0 & 0 & 0 \end{pmatrix}$. By theorem G1, the $d_{i,i}$ are the invariant factors of N/E. $(A - xI)Q = P^{-1}B$ and $P^{-1}B$ is just the ith column of $P^{-1}b_{i,i}$. So the basis for M is just the columns of Q and the basis for N is just the columns of P^{-1}, namely,

$y_1, y_2, \ldots, y_n$. Again, by theorem G1, $N/E = \oplus_{\{s+1 \le i \le n\}} R(y_i + E)$. The isomorphism in G3, θ, is given by $\theta(y_i + E) = \sum_j y_{ji} v_j = u_i$, since $y_i = \sum_j y_{ji} e_j$. Finally, we get, $V_T = \oplus_{\{s+1 \le i \le n\}} R\langle u_i \rangle$. This gives the RCF.

Example: $F = \mathbb{Q}$ and T is represented over the standard basis as

$$A = \begin{pmatrix} 5 & -8 & 4 \\ 6 & -11 & 6 \\ 6 & -12 & 7 \end{pmatrix}$$

then

$$P = \begin{pmatrix} 1 & 0 & 0 \\ -\frac{3}{2} & 1 & 0 \\ \frac{x+5}{4} & -2 & 1 \end{pmatrix},\ Q = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & \frac{3}{2} \\ 1 & 2 & \frac{x+7}{4} \end{pmatrix},\ P(A - xI)Q = \begin{pmatrix} 4 & 0 & 0 \\ 0 & (1-x) & 6 \\ 0 & 0 & \frac{1-x^2}{4} \end{pmatrix}$$

Now compute P^{-1}, columns not containing x and their images under A will be the basis for the matrix in rational canonical form.

$$P^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ \frac{3}{2} & 1 & 0 \\ \frac{7-x}{4} & 2 & 1 \end{pmatrix}.$$

In this example, $V_T \cong Rw_1 \oplus Rw_2 \oplus Rw_3$ with $w_1 = e_3$, $w_2 = Tw_1 = (4, 6, 7)^T$, $w_3 = e_2 + 2e_3$ and so the basis change matrix is

$$L = \begin{pmatrix} 0 & 4 & 0 \\ 0 & 6 & 1 \\ 1 & 7 & 2 \end{pmatrix}.$$

$$L^{-1}AL = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Since $m_T(x)$ has linear factors, the Jordan canonical form is diagonal and

$$J = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

One more example: $F = \mathbb{Q}$ and T is represented over the standard basis as

$$A = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}.$$

$m_T(X) = x^2 - (\lambda_1 + \lambda_2)x + \lambda_1\lambda_2$ is the minimal polynomial. Further,

$$A - xI = \begin{pmatrix} \lambda_1 - x & 0 \\ 0 & \lambda_2 - x \end{pmatrix},\ P(A - xI)Q = \begin{pmatrix} 1 & 0 \\ 0 & (x - \lambda_1)(x - \lambda_2) \end{pmatrix},$$

with

$$P = \frac{1}{\lambda_1 - \lambda_2} \begin{pmatrix} -\lambda_2 & \lambda_1 \\ 1 & -1 \end{pmatrix},\ P^{-1} = \begin{pmatrix} 1 & \lambda_1 \\ 1 & \lambda_2 \end{pmatrix}$$

So the basis for the RCF is $\langle (1, 1)^T, (\lambda_1, \lambda_2)^T \rangle$. To switch basis, $v_{[e]} = Lv_{[f]}$. The matrix, L, is then

$$L = \begin{pmatrix} 1 & \lambda_1 \\ 1 & \lambda_2 \end{pmatrix},\ L^{-1} = \frac{1}{\lambda_1 - \lambda_2} \begin{pmatrix} -\lambda_2 & \lambda_1 \\ 1 & -1 \end{pmatrix}.$$

We see that

$$L^{-1}AL = \begin{pmatrix} 0 & -\lambda_1\lambda_2 \\ 1 & \lambda_1+\lambda_2 \end{pmatrix}$$

which is the RCF.

Principal Component Analysis: $P_A = A(A^TA)^{-1}A^T$ where the rank of A is the number of columns, is the symmetric projector; $P_{A^\perp} = I - P_A$. $P_A^2 = P_A$, $P_{A^\perp}^2 = P_{A^\perp}$, $P_A^T = P_A$, $P_{A^\perp}^T = P_{A^\perp}$. $S = AA^T$ is invertible. $P_{\vec{a}}(\vec{w})$ is the projection of $\vec{w}$ along $\vec{a}$. The linear system $A\vec{f} = P_A\vec{b}$ has solution $\vec{f} = A^{-1}P_A\vec{b}$ the least squares approximation of data points (x_i, y_i) can be calculated from this too. *Example:* Fit $f(x) = f_0 + xf_1$ to the data $(-1,1),(0,0),(1,2)$ by solving $\begin{pmatrix} 1 & -1 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}(f_0,f_1)^T = (1,0,2)^T$. In general, the least squares approximation arises from the symmetric projection in the sample space $\mathbb{R}^s$ where s is the number of data points. $f(A)\vec{v} = (f_0 + f_1A + \ldots + f_nA^n)\vec{v} = (\vec{v}, A\vec{v}, \ldots, A^n\vec{v})$. Vandermonde determinant and Fourier $V(x_0, x_1, \ldots, x_n)$ where the x_i are roots of $x^{n+1} - 1 = 0$. $Z(x) = (x - x_j)Z_j(x)$ solves for coefficients $f_0, f_1, \ldots, f_n$ using Lagrange interpolants $\Lambda_j(x) = \frac{Z_j(x)}{Z_j(x_j)}$. For PCA, $\mu_A(x) = (x-\lambda_1)^{m_1}(x - \lambda_2)^{m_2}\ldots(x-\lambda_t)^{m_t}$. There are polynomials in A, denoted $A_{\lambda_1}A_{\lambda_2}\ldots A_{\lambda_t}$ such that $(A-\lambda_iI)^mA_{\lambda_i} = 0$ and $A = A_{\lambda_1}A_{\lambda_2}\ldots A_{\lambda_t}$. The A_{λ_i} are called components. The list of basic eigenvectors of A form the columns of the diagonalizing matrix, P and $AP = PD$; A is diagonalizable when P is invertible. Approximating a rank r $n \times n$ matrix requires $2nr$ terms. *Mean clustering:* replace M with $D = diag(\alpha_1, \ldots, \alpha_i)$ where $\alpha_i = \sqrt{\frac{1}{(MM^T)_{ii}}}$. How closely can a scatterplot be approximated by a line A with direction $\vec{a}$? Find the vector $\vec{a}$ that maximizes $|P_{\vec{a}}(\vec{m_1})|^2 + |P_{\vec{a}}(\vec{m_2})|^2 + |P_{\vec{a}}(\vec{m_s})|^2 = (\vec{a}^T\vec{m}_1)^2 + (\vec{a}^T\vec{m}_2)^2 + \ldots(\vec{a}^T\vec{m}_t)^2$. Maximize $\vec{a}^TMM^T\vec{a}, \forall\vec{a} \in \mathbb{R}^s, |\vec{a}| = 1$. $C = MM^T$ is a correlation matrix with c_{ij} is the correlation of i, j; if $u_i \perp u_j$ they are uncorrelated. $\exists P : CP = PD$, $MM^T = C = PDP^{-1}$ and maximize $\vec{u}^TD\vec{u}, |\vec{u}| = 1$, $\vec{u} = P^T\vec{a} \in \mathbb{R}^s$. C is diagonalized by $P : PP^T = I$.

1.2.5 Bilinear Forms and Classical Groups

Definition: A *pairing*, $(W, V) \to k$ is a bilinear map. If $V_0 \subset V$, $V_0^* = \{\vec{w} \in W : (\vec{w}, \vec{v_0}) = 0, \forall\vec{v_0} \in V_0\}$, $v_0 \subset (V_0^*)^*$. V^* is called the left kernel. Same holds *mutatis mutandis* for $W_0 \subseteq W$ provided $W^* = 0$ is the right kernel. If $(W, V) \to k$ is a pairing with left kernel 0 and $\vec{w} \in W$, define $\varphi_{\vec{w}}(\vec{v}) = (\vec{w}, \vec{v})$. $\varphi_{\vec{w}} \in \hat{V}$ and the map $\vec{w} \mapsto \varphi_{\vec{w}}$ is an injection from $W \to \hat{V}$. Similarly, if the right kernel is 0, there is an injection $V \to \hat{W}$.

If $W_0 \subseteq W$, $codim_W(W_0) = dim(W) - dim(W_0)$. If $W_0 \subset W$, $V_0 \subset V$ and $V^* = 0$, there are natural injective morphisms $V/W_0^* \to \hat{W_0}$ and $V_0^* \to \hat{V/V_0}$. Thus, $dim(V/W_0^*) \leq dim(\hat{W_0}) = dim(W_0)$ and $dim(W_0^{**}) \leq codim(W_0^*) \leq dim(W_0)$. If $W = \hat{V}$, both kernels are 0. If (W, V) is a pairing, (a) $dim(W/V^*) = dim(V/W^*)$, (b) if $V^* = 0$, $dim(W_0^{**}) = codim(W_0^*) = dim(W_0)$ and if W_0 is finite dimensional, $W_0^{**} = W_0$ and W_0 and V/W_0^* are naturally dual, (c) If $V^* = 0$ and $W^* = 0$, and V and W are finite dimensional, V and W are naturally dual and there is a 1-1, inclusion reversing correspondence of subgroups of V and W under the $*$ operator: $W_0 \leftrightarrow W_0^*$.

Let $A = (a_{ij})$ be an $m \times n$ matrix with entries in k and $\vec{x} = (x_1, \ldots, x_n)^T$. Let $\vec{b} = (b_1, \ldots, b_m)^T$ then $A\vec{x} = \vec{b}$ is a system of linear equations. Set $x = E_1x_1 + E_2x_2 + \ldots + E_nx_n, E_i \in V = k^n$. Suppose $\hat{V}$ is dual to V with basis $\varphi_1, \ldots, \varphi_n$: $\varphi_jE_k = \delta_{jk}$. Let $\psi_i(x) = (a_{i1}\varphi_1 + \ldots + a_{in}\varphi_n)(E_1x_1 + \ldots + E_nx_n) = a_{i1}x_1 + \ldots + a_{in}x_n$. $W \subset \hat{V}$, $W = \langle\psi_j(x)\rangle$ and $dim(W) =$ row rank. S_m is the $m-$tuple column vectors with entries in k. Note that if A_i are column vectors forming A, they are in the column space of A as is $\vec{b}$ and

$A_1x_1 + \ldots + A_nx_n = \vec{b}, \vec{b} = (\psi_1(x), \ldots, \psi_m(x))$. If $f : V \to S_m, f(x) = (\psi_1 x, \ldots, \psi_n x)$, $ker(f) = W^*$. If $Im(f) = U$, $U \cong V/W^*$ and $dim(U) = codim(W^*) = dim(W)$. This shows the row rank equals the column rank.

Let $B_{ij}(\lambda) = I + \lambda(\delta_{il}\delta_{jk})_{lk}$. If $A \in GL_n(k), A = BD(\lambda)$ where $B \in SL_n(k)$ and $D(\lambda)$ is the same as the identity except for λ in the lower rightmost position. Put $Z = Z(k), S = \langle x^2, x \in k \rangle$ (as an additive group). If $x^2 \in Z, \forall x$ then k is commutative; further, unless k is commutative and $char(k) = 2$, $S = k$.

Definition: $\tau \in GL_n(k)$ is a *transvection* if $\exists H = \{h : \varphi(h) = 0, \varphi \in \hat{V}\}$ with $\tau(h) = h, h \in H$ and $\tau(x) - x \in H, \forall x \in V$. If τ is a transvection with hyperplane H, pick $\vec{b} : \varphi(\vec{b}) = a \neq 0$, set $\tau(x) = x - \vec{b}a^{-1}\varphi(x)$ then $\tau(t(x)) = t(x)$, thus $\tau(x) = x + \vec{a}\varphi(x)$ with $\vec{a} = \tau(\vec{b}a^{-1}) - \vec{b}a^{-1}$. So all transvections are of this form.

Theorem: $B_{ij}(\lambda)$ is a transvection. If $\vec{a}, \vec{b} \in H$ then $\tau_{\vec{a}}(\tau_{\vec{b}}(x)) = \tau_{\vec{a}+\vec{b}}(x)$. If $\sigma \in GL_n(k)$ and τ is a transvection, so is $\tau' = \sigma\tau\sigma^{-1}$ and $\tau'(x) = x + (\sigma(A))\varphi(\sigma^{-1}(x))$; conversely, if $\tau''(x) = x + \vec{a'}\psi(x)$ is another transvection with hyperplane H', we show $\exists\sigma$: $\sigma(H) = H'$ and $\sigma(\vec{a}) = a'$ and thus that all transvections are conjugate and hence have the same determinant.

Proof: Pick $\vec{b}, \vec{b'}$ with $\varphi(\vec{b}) = \psi(\vec{b'}) = 1$. $\exists\sigma : \sigma(\vec{a}) = \vec{a'}, \sigma(H) = H', \sigma(\vec{b}) = \vec{b'}$. Then $\tau''(x) = x + \vec{a'}\varphi(\sigma^{-1}(x))$, $\exists c : \phi(x) = \varphi(\sigma^{-1}(x))$, setting $x = \vec{b'}, \sigma^{-1}(x) = \vec{b}$ we get $c = 1$ and $\tau'' = \tau'$. If H has at least three vectors then $\exists\vec{a}, \vec{b}, \vec{c}$ with $\vec{c} = \vec{a} + \vec{b}$ and $\tau_{\vec{a}}(\tau_{\vec{b}}(x)) = \tau_{\vec{c}}(x)$ and since they all have the same determinant, it must be 1. In that case, $f : GL_n(k) \to GL_n(k)/GL_n(k)'$, $f(\sigma\tau\sigma^{-1}) = f(\tau)$ so all transvections have the same image under f and $\tau \in GL_n(k)' = SL_n(k)$. If $n \geq 3$ H and H' have independent vectors and we can choose $\sigma : det(\sigma) = 1$ so the transvections are conjugate in $SL_n(k)$. Finally, the center of $SL_n(k)$ consists of the matrices αI with $\alpha^n = 1$. We can conclude: If G is a normal subgroup of $GL_n(k)$ containing a transvection and $n \geq 3$ or $n = 2$ and $|k| \geq 4$ then $SL_n(k) \subseteq G$ if $G > Z(GL_n(k))$.

Theorem: If v, w are linearly independent, there is a transvection, T: $Tv = w$.

Proof: $W = \{x : x \cdot (v - w) = 0\}$, $x, y \notin$. $T_{|W|} = 1$, $T(v) = w$.

Theorem: If W_1, W_2 are hyperplanes in V, and $v \in V \setminus W_1 \cup W_2$, there is a transvection, T: $T(W_1) = W_2, T(v) = v$.

Proof: $V = W_1 + W_2$. $dim(W_1 \cap W_2) = n - 2$. $\exists x \in W_1, y \in W_2 : v = x + y$. $V = W_1 \cap W_2 + Fx + Fy$. Define $T_{W_1 \cap W_2 + F(x+y)} = 1$ and $T(x) = y$.

Theorem: All transvections are $GL(V)$ conjugate. If T_1, T_2 are transvections on V, $n = dim(V) \geq 3$ and T_1 and T_2 are $GL(V)$ conjugate then they are $SL(V)$ conjugate.

Proof: Transvections are all of the form $T = 1 + \lambda B_{mn}$ with $B_{mn} = (\delta_{mi}\delta_{nj})$. B_{lm} is conjugate to B_{kn} via permutation matricies. Suppose, for example that $T = 1 + \lambda_1 B_{mn} = \begin{pmatrix} 1 & \lambda_1 \\ 0 & 1 \end{pmatrix}$. Put $S = \begin{pmatrix} \frac{1}{\lambda_1} & -1 \\ 0 & \frac{1}{\lambda_2} \end{pmatrix}$, then $S^{-1}TS = \begin{pmatrix} 1 & \lambda_2 \\ 0 & 1 \end{pmatrix}$. So all transvections are conjugate in $GL(V)$. If $n \geq 3$, we can pick a diagonal element so that $det(S) = 1$ and preserve the conjugacy.

Theorem: If $dim(V) \geq 3$, the transvections on V generate $SL(V)$. $SL(V)' = SL(V)$ and $PSL(V)' = PSL(V)$.

Proof: It suffices to show there is a (non-trivial) transvection in $SL(V)'$ since they are all conjugate. Define $T_1(v_1) = v_1 - v_2, T_1(v_j) = v_j, j \neq 1$ and $T_2(v_2) = v_2 - v_3, T_1(v_j) = v_j, j \neq 2$. $T_1T_2T_1^{-1}T_2^{-1}$ is a transvection.

Theorem: $PSL(V)$ is 2-transitive on $P_{n-1}(V)$.

Proof: Let $[v_1] \neq [v_2], [w_1] \neq [w_2] \in P_{n-1}(V)$. We can choose basis $\langle v_1, v_2, v_3, \ldots, v_n\rangle$ and $\langle w_1, w_2, v_3, \ldots, v_n\rangle$. Define T_b by $T_b(v_1) = bw_1$ $T_b(v_2) = w_2$, and $T_b(v_i) = v_i, i \geq 3$. Finally, pick b: $det(T_b) = 1$.

Pairings and isometries: Let $V \times V \to k$ be a pairing with trivial left and right kernels. σ is an *isometry* if $(x, y) = (\sigma x, \sigma y), \forall x, y \in V$. $det(\sigma)^2 = 1$ for all isometries; if $det(\sigma) = 1$, σ is a rotation, if $det(\sigma) = -1$, σ is a reflection. A quadratic map, Q satisfies $Q(ax) = a^2Q(x)$ and $(x, y) = Q(x+y)-Q(x)-Q(y) = (y, x)$ is a pairing. If $char(F) \neq 2$, $Q(x) = \frac{1}{2}(x, x)$. Pairings arising from quadratic maps are symmetric. $\vec{a} \perp \vec{b} \leftrightarrow (\vec{a}, \vec{b}) = 0$. If $\langle v_1, v_2, \ldots, v_n\rangle$ span V and $(\vec{v_i}, \vec{v_j}) = g_{ij}$ and if $\langle u_1, u_2, \ldots, u_n\rangle$ is another basis related to the original by $u_i = \sum_j a_{ji}v_j$ then $\overline{g_{ij}} = A^TGA$, where $G = (g_{ij})$. The form is symmetric if $a_{ij} = a_{ji}$, antisymmetric if $a_{ij} = -a_{ji}$.

Isotropic spaces Let $V^* = rad(V) = V \cap V^\perp$ and $V = rad(V) \oplus U$, $U \cong V/rad(V)$. Suppose V is non-singular and $U \subset V$ then $U^{**} = U, dim(U) + dim(U^*) = dim(V)$ and $rad(U) = rad(U^*) = U \cap U^*$. The subspace U is non-singular iff U^* is non-singular and then $V = U \perp U^*$. A vector $\vec{v}$ is isotropic if $(\vec{v}, \vec{v}) = 0$. U is isotropic if $(u_1, u_2) = 0, \forall u_1, u_2 \in U$. There are two geometries for symmetric metric spaces: (1) *symplectic* if $(\vec{v}, \vec{v}) = 0, \forall \vec{v} \in V$ and $(x, y) = -(y, x)$; (2) *orthogonal* if $(x, y) = (y, x), \forall x, y \in V$. If V is orthogonal and every vector is *isotropic* then V is isotropic.

Definitions: Suppose $dim(V) = 2$ and V is non-singular but has an isotropic vector, $\vec{n}$ then $\exists \vec{m} : \vec{n}^2 = \vec{m}^2 = 0, \vec{n}\vec{m} = 1$, $V = \langle \vec{n}, \vec{m}\rangle$. ($V = \langle \vec{n}, \vec{a}\rangle$ for some $\vec{a}$. Set $\vec{m} = x\vec{n} + y\vec{a}$; if $\vec{n}\vec{a} = 0$, V is singular so we can find $y : y\vec{n}\vec{a} = 1$. Can also find $x : \vec{m}^2 = 0$.) $\langle \vec{n}, \vec{m}\rangle$ is a *hyperbolic plane.* A non-singular space, V, with orthogonal geometry is an orthogonal sum of lines. A non-singular space, V, with symplectic geometry is an orthogonal sum of hyperbolic planes.

Witt's Theorem: Let V and W be isometric via ρ. Let $\sigma : V_0 \to W_0$ be an isometry for $V_0 \subset V$ and $W_0 \subset W$, then σ can be extended to an isometry of V. O_n: isometries.

Proof:

Definitions: O_n^+: rotations, O_n^-: reflections. $\Omega_n = O_n'$. If V is a vector space with over $\mathbb{R}$ with a positive definite form (resp. $\mathbb{C}$ with a hermitian form) and W is a subspace of V then $V = W \oplus W^\perp$. $V^* \otimes V \to \mathcal{L}(V, V)$ via $L_{\phi\otimes v}(w) = \phi(w)v$. If n is odd, $1_V = Z(O_n^+)$. If n is even, $\pm 1_V = Z(O_n^+)$. If $n = 2$ over F_q, the plane contains $q + 1$ lines: $\langle A + xB\rangle, \langle B\rangle$; if V is isotropic, $\epsilon = 1$, otherwise V contains no isotropic vectors and $\epsilon = -1$. There are $q - \epsilon$ non-isotropic lines. $O(V)$ has $q - \epsilon$ elements. Let φ_n be the number of isotropic vectors in V and λ_n the number of hyperbolic pairs. If $\langle N, M\rangle$ is a hyperbolic plane, $\langle N, M\rangle \oplus \langle N, M\rangle^* = V$. $\langle N^*\rangle$ contains $q\varphi_{n-2}$ isotropic vectors. A type I form: TBD. Type I, II form: $\varphi_n = q^{n-1}$. Type III, IV form: $\varphi_n = q^{n-1} + cq^{\frac{n}{2}}$, $n \geq 1$. If $\Phi_n = |O_n^+(q)|$ or $|PSp_n(q)|$, $\Phi_n = \lambda_n\Phi_{n-2}$.

Classical Groups Summary. Theorem: Every isometry in $\mathbb{R}^n$ is the product of $\leq n + 1$ reflections.

Proof: It suffices to show every isometry, f with $f(0) = 0$ is the product of at most n reflections. This is true for $n = 1, 2$, suppose it is true for $n - 1$. $||f(e_n) - f(0)|| = ||f(e_n)|| = ||e_n|| = 1$. There is a reflection, R such that $g = Rf$ fixes 0 and e_n and hence $L = \{te_n\}$. Put $W =$

$\{(x_1, \ldots, x_{n-1}, 0), x_i \in \mathbb{R}\}$. $W \perp L$ and g fixes scalar products. If $g(x) = y$, $\pi_n(x) = \pi_n(y)$. Regard g as a map on $\mathbb{R}^{n-1}$. $g^*(x_1, \ldots, x_{n-1}) = (y_1, \ldots, y_{n-1})$. By induction, $g^* = R_1^* \ldots R_{n-1}^*$ with $R_j^*(x) = x - 2(x, a_j^*)a_j^*, ||a_j^*|| = 1$. Put $R_j(x) = x - 2(x, a_j)a_j$, $a_n = 0, a_j^* = a_j, j < n$. $f = RR_1 \ldots R_{n-1}$.

If G is one of $SL(V)$, $Sp(V)$, $SO(V)$ or $S\Omega(V)$, $G = BWB$, where B is the *Borel subgroup* (upper triangular matrices) and W is the *Weyl subgroup* (the permutation matrices).

1.2.6 Fields

Theorem: If α is the root of an irreducible polynomial $p(x) \in F[x]$ then $F(\alpha) = F[\alpha] = F[x]/(p(x))$ (This is called a *field extension*). Isomorphisms between fields can be extended to isomorphisms of extensions over associated (under the isomorphism) polynomials.

Proof: Suppose $\sigma : F \to K$ then the natural extension of σ to $F[x]$ gives $\sigma : F[x] \to K[x]$. If $p(x)$ is irreducible, this isomorphism can be extended uniquely to $F[x]/(p(x)) \to K[x]/(p^\sigma(x))$.

Theorem: Any two splitting fields of the same polynomial over F are isomorphic.

Proof: Let α and β be two roots of and irreducible polynomial which divides a $f(x)$; let E be the splitting field of $f(x)$. There is an isomorphism from $F(\alpha)$ into $F(\beta)$ which can be extended to an automorphism of E.

Definitions: Let E be a field and G be a set of automorphisms of E, $E_G = \{x \in E : \varphi(x) = x, \forall \varphi \in G\}$. Note that E_G is a field. A polynomial is *separable* if the roots of every irreducible factor are distinct. An extension E/F is *separable* if every element of E is the root of a separable polynomial in $F[x]$. E is a *Galois* over F if $E_G = F$. E is *normal* over F if an irreducible polynomial over F with one root in E, *splits*.

Artin's Lemma: Distinct automorphisms are linearly independent.

Proof: Suppose not. Let $c_1\phi_1(x) + c_2\phi_2(x) + \ldots + c_r\phi_r(x) = 0$ be a minimal relation. Since the automorphisms are distinct, $\exists \beta : \phi_1(\beta) \neq \phi_r(\beta)$. Obtain two equations from the minimal relation, the first by substituting βx into the equation for beta, the second by multiplying the equation by $\phi_r(\beta)$, then subtract them. This is a shorter relation.

Theorem: If G is a finite set of automorphisms fixing F, then $r = |E : F| \geq |G| = n$.

Proof: Suppose not. Let $\{\omega_1, \ldots, \omega_r\}$ be a basis for E over F. Consider the r equations: $\phi_1(\omega_k)x_1 + \ldots + \phi_n(\omega_k)x_n = 0$ for $k = 1, 2, \ldots r$. Since $n > r$ there is a non trivial solution $c_1, c_2, \ldots, c_n$. Let $x = \sum_{i=1}^r a_i\omega_i$. Multiply the first equation by a_1, the second by a_2 and so on then add them to get $c_1\phi_1(x) + c_2\phi_2(x) + \ldots + c_n\phi_n(x) = 0$ for all x. This contradicts the Artin's result.

Theorem: Let $G = \{\phi_1, \phi_2, \ldots, \phi_n\}$ be a finite group of $Aut(E)$ and $F = E_G$, then $r = [E : F] = |G| = n$.

Proof: Suppose $r > n$. Let $\{\omega_1, \ldots, \omega_r\}$ be a basis for E over F. Consider the n equations: $\phi_k(\omega_1)x_1 + \ldots + \phi_k(\omega_r)x_r = 0$ for $k = 1, 2, \ldots, n$. This has a non trivial solution, $\langle c_1, c_2, \ldots, c_r\rangle$, with $r - n$ more unknowns than equations. Let $\langle c_1, \ldots, c_r\rangle$ be a solution with the minimum number of non-zero elements. We may reorder the coefficients and basis so $c_1 \neq 0$ and by dividing each of the linear equations by c_1, we may assume $c_1 = 1$. We claim each $c_i \in F, \forall i$. If not, say $c_2 \notin F$. Then $\exists \phi_k : \phi_k(c_2) \neq c_2$. Thus, $\sum_{i=1}^r c_i\phi_j(\omega_i) = 0$ and $\sum_{i=1}^r \phi_k(c_i\phi_j(\omega_i)) = 0$ for each $1 \leq j \leq n$. Again, reordering, $\sum_{i=1}^r \phi_k(c_i)\phi_j(\omega_i) = 0$ for each $1 \leq j \leq n$. Subtracting

the two equations, we get a non-trivial linear relation with fewer non-zero coefficients. So, $c_i \in F, \forall i, 1 \leq i \leq r$. This gives a non-trivial linear dependence in F among the ω_i which contradicts their linear independence, so $r \leq n$. Now $r \geq n$ by the previous result so $n = r$.

Primitive Element Theorem: If $E = F[\alpha_1, \ldots, \alpha_n]$ with $\alpha_2, \ldots, \alpha_n$ separable then $E = F[\alpha]$, some α. Every separable finite extension is primitive.

Proof: Assume F is not finite, $E = F[\alpha, \beta]$ with f, g the minimal polynomials for $\alpha = \alpha_1$ and $\beta = \beta_1$ respectively, α_i the roots of f and β_i the roots of g. Let E be the splitting field of $f(x)g(x)$. $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$ has one root for each i, k; pick c such that $\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1$ and set $\theta = \alpha + c\beta$. Claim: $E = F[\theta]$. $f(\theta - c\beta) = g(\beta) = 0$ so $(f(\theta - cx), g(x)) = (x - \beta) \in F[\theta][x]$.

Theorem: Let E be a splitting field for $f(x)$ over $F[x]$. If $p(x)$ is irreducible and has one zero in E, then $p(x)$ splits in E.

Proof: Let L be the splitting field of $f(x)p(x)$. Set $E = F(a_1, a_2, \ldots, a_n)$ where $a_1, a_2, \ldots, a_n$ are the roots of $f(x)$. Suppose $p(\alpha) = 0, \alpha \in E$ and $p(\beta) = 0$. Let $\sigma : F(\alpha) \to F(\beta)$ be an isomorphism with $\sigma(\alpha) = \beta$. Extend σ to $\tau : L \to L$. τ permutes the roots of $f(x)$ so $\tau(E) = E$. $\alpha = \frac{m(a_1, a_2, \ldots, a_n)}{n(a_1, a_2, \ldots, a_n)}$. So $\beta = \tau(\alpha) = \tau(\frac{m(a_1, a_2, \ldots, a_n)}{n(a_1, a_2, \ldots, a_n)}) \in E$.

Theorem: Let E be a finite extension of F, $char(F) = 0$. If E is a splitting field of $f(x) \in F[x]$ then $|\mathcal{G}(E/F)| = [E : F]$.

Proof: $E = F(w)$, $p(w) = 0$ and p splits by foregoing. $deg(p) = [E : F] = |G|$.

Theorem: Let $F \subseteq E$, $char(F) = 0$. If $G = \mathcal{G}(E/F)$ fixes F then E is a normal extension iff F is the fixed field of G.

Proof: $E = F(w)$, $|G| = [E : F]$. Let $K = \{a : \sigma(a) = a, \forall \sigma \in G\}$. $F \subseteq K \subseteq E$ and $E = K(w)$. STS if g is irreducible over F and $g(w) = 0$ then g is irreducible over K. Let p be an irreducible polynomial for w over K. Applying elements of G, each root of p is a root of g.

Theorem: Let E be a normal extension of F. $E \supset K \supset F$. If $\mathcal{G}(E/F) > S$ has K as a fixed field then $\mathcal{G}(E/K) = S$.

Proof: Suppose $S \subseteq \mathcal{G}(E/K) = T$. By a previous result $|T| = |S|$ so $S = T$.

Lemma: Let K be the splitting field of $f(x)$ over k and let $p(x)$ an irreducible factor of $f(x)$, if the roots of $p(x)$ are $\alpha_1, \ldots, \alpha_r$, there is a $\sigma_i \in \mathcal{G}(K/k)$ such that $\sigma_i(\alpha_1) = \alpha_i$.

Proof: This follows from the isomorphism $F[x]/(f(x)) \to F(\alpha)$ and $F[x]/(f(x)) \to F(\alpha_i)$.

Theorem: E is Galois over F iff (i) every irreducible polynomial in $F[x]$ with one root in E splits and (ii) $E = F(\theta)$. $GF(p^m) \subseteq GF(p^n)$ iff $m|n$.

Proof: Let $\theta = \theta_1$ and $\varphi = \varphi_1$ is another root. Let $f \in F[x]$ be irreducible with root θ. By the lemma, there is a $g \in \mathcal{G}(E/F)$. $f^g(x) = f(x)$. (ii) follows from this. $\theta^g = \varphi$ and so φ is thus a root of f.

Theorem: The following are equivalent: (1) E is a splitting field over F of a separable polynomial $f(x)$. (2) $F = E_G$. (3) E is finite dimensional, normal and separable. Moreover, if E and F are as in (1) and $G = \mathcal{G}(E/F)$ then $F = E_G$ and if F and G are as in (2) then $G = \mathcal{G}(E/F)$.

Proof of (1 → 2): $G = \mathcal{G}(E/F)$ and $F' = E_G$. $F \subseteq F' \subseteq E$. E is a splitting field over F' of $f(x)$ as well as over F and $G = \mathcal{G}(E/F')$. $[E : F] = |G| = [E : F']$ so $F = F'$ and $F = E_G$

Proof of (2 → 3): By Artin $[E : F] \leq |G|$ so E is finite dimensional over F. Let $f(x) \in F[x]$ having root $r \in E$ be irreducible. Let $\langle r = r_1, \ldots, r_m \rangle$ be an orbit of r under G. For $\eta \in G$, $(\eta(r_1), \ldots, \eta(r_m))$ is a permutation of $(r_1, r_2, \ldots, r_m)$. $f(r_i) = 0, 1 \leq i \leq m$ and $(x - r_i) \mid f(x)$ so $g(x) = \prod_{i=1}^{m}(x - r_i) \mid f(x)$. Apply to $g(x)$ the automorphism of $E[x]$ which sends $x \mapsto x, a \mapsto \eta(a)$ for $a \in E$. This gives $\eta(g(x)) = \prod_{i=1}^{m}(x - \eta(r_i)) = g(x)$. Since this holds for every $\eta \in G$, the coefficients of g are $G-$invariant hence $g(x) \in F[x]$. Since $g(x)$ is irreducible in $F[x]$, $f(x) = g(x) = \prod_{i=1}^{n}(x - r_i)$ a product of linear factors in $E[x]$. Thus E is separable and normal over F and (3) holds.

Proof of (3 → 1): Since $[E : F] < \infty$ so $E = F(r_1, r_2, \ldots, r_k)$ and r_i is algebraic over F. Let f_i be the minimal polynomial for r_i. By hypothesis, $f_i(x)$ is a product of linear factors in $E[x]$. It follows that $f(x) = \prod_{i=1}^{n} f_i(x)$ is separable and $E = F(r_1, r_2, \ldots, r_k)$ is a splitting field for E over F and (1) follows.

Proof of supplement: To prove the second part of the supplement, under the hypothesis of part (2) of the supplement,$[E : F] \leq G$ and since (3) holds, $\mathcal{G}(E/F) = [E : F]$. Since $G \subseteq \mathcal{G}(E/F)$ and $|G| \geq [E : F] = |\mathcal{G}(E/F)|$, $G = \mathcal{G}(E/F)$.

Galois' Theorem: Let K be a normal, separable extension of k. Let $G = \mathcal{G}(K/k)$, $H < G$, $K \supseteq F \supseteq k$. There is a bijective pairing between H and F, such that (i) $H_1 \supseteq H_2 \leftrightarrow K_{H_2} \supseteq K_{H_1}$; (ii) $|H| = [K : K_H]$, $[G : H] = [K_H : k]$; and, (iii) $H \lhd G \leftrightarrow K_H$ is normal over k and $\mathcal{G}(K_H/k) = G/H$.

Proof:

Let $H < G = \mathcal{G}(K/k)$. $k = K_G$. Put $F = K_H$. $k \subseteq F \subseteq K$. By the previous result, $|\mathcal{G}(K/K_H)| = |H| = [K : K_H]$. Applying supplementary result (2) above with H in place of G, we get $\mathcal{G}(K/K_H) = H$. Similarly, $|H| = |\mathcal{G}(K/K_H)| = [K : K_H]$.

Now, let F be any intermediate subfield between K and k and $H = \mathcal{G}(K/F)$. $H \subseteq G = \mathcal{G}(K/K_H)$. K is a splitting fields over F of a separable polynomial since it is a splitting field over k of a separable polynomial. The supplementary result of (1) above applied to K and F shows $F = K_H = K_{\mathcal{G}(K/F)}$. Thus the map between F and K_H are inverses.

If $H_1 \supseteq H_2$ then $K_{H_1} \subseteq K_{H_2}$. Moreover, if $K_{H_1} \subseteq K_{H_2}$ then we also have $H_1 = \mathcal{G}(K/K_{H_1}) \supseteq \mathcal{G}(K/K_{H_2}) = H_2$. Hence (i) holds.

The first part of (ii) follows as before. $|G| = [K : k] = [K : K_H][K_H : k] = |H|[K_H : k]$ and $|G| = [G : H]|H|$ so $[K_H : k] = [G : H]$. This proves (ii).

If $H < G$ and $F = K_H$, the subfield corresponding to $\eta H \eta^{-1}$ is $\eta(F)$. $\eta H \eta^{-1} \eta F = \eta(F)$, so $H \lhd G$ iff $\eta(F) = F, \forall \eta \in G$. If this holds, every η, maps F to itself and $\eta_{|F} = \overline{\eta}$ is an automorphism of F/k. Thus the restriction $\eta \to \overline{\eta}$ of $\mathcal{G}(K/k)$ into $\mathcal{G}(F/k)$ is a homomorphism. The image $\overline{G}$ is a group of automorphisms of F and $K_{\overline{G}} = k$. Hence $\overline{G} = \mathcal{G}(F/k)$. The kernel of the map $\eta \to \overline{\eta}$ is the set $\{\eta \in G : \eta_{|F} = 1_F\}$; by the pairing, $\mathcal{G}(K/F) = H$. This kernel is H and $\overline{G} = \mathcal{G}(F/k) \approx G/H$. Since $k = K_{\overline{G}}$, F is normal over k.

Conversely, suppose F is normal over k. Let $a \in F$ and let $f(x)$ be the minimal polynomial for a over k then $f(x) = (x-a_1)(x-a_2)\dots(x-a_n) \in k[x]$ where $a = a_1$. If $\eta \in G$ then $f(\eta(a)) = 0$ which implies $\eta(a) = a_i$ for some i so $\eta(a) \in F$. Therefore, $\eta(F) \subseteq F$. $\eta H \eta^{-1} \subseteq H$ if H is the subgroup corresponding to F in the Galois pairing. Thus $H \lhd G$, concluding the proof of (iii).

Theorem: If $f(x)$ is solvable by radicals, the Galois group of its splitting field is *solvable*. Galois group of an equation is a permutation group on its roots. Splitting field of $g(x) = 2x^5 - 10x + 5$ is S_5.

Proof: There is an element of order 5 in G since $g(x)$ is irreducible. Complex conjugation is an automorphism of order 2. These generate S_5.

Computing the Galois group for an arbitrary polynomial: Suppose, $f(t) = t^n - s_1 t^{n-1} + \ldots + (-1)^n s_n$ over the field k. Let K be the splitting field of f over k and $G = \mathcal{G}(K/k)$. Assume $f(t)$ has distinct zeros $\alpha_1, \dots, \alpha_n$ and consider the indeterminates $x_1, \dots, x_n$. The s_k are elementary symmetric polynomials in the α_k. Put $\beta = \sum_{j=1}^n x_j \alpha_j$. Suppose $\sigma \in S_n$. We set $\sigma_x(\beta) = \sum_{j=1}^n x_{\sigma(j)} \alpha_j$ and $\sigma_\alpha(\beta) = \sum_{j=1}^n x_j \alpha_{\sigma(j)}$. Put $q(t) = \prod_{\sigma \in S_n} (t - \sigma_x(\beta)) = \sum_{j=0}^{n!} g_i(s_1, \dots, s_n) x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} t^j$. Now $q(t) = q_1(t) q_2(t) \dots q_k(t)$ where each $q_k(t)$ is irreducible. We can assume $(t - \beta) \mid q_1(t)$. Put $G_1 = \{\sigma \in S_n : q_1(t)^\sigma = q_1(t)\}$. In fact, if we put $S_{(1)} = \{\sigma : (t - \sigma_x(\beta)) \mid q_1(t)\}$, $S_{(1)} = G_1$. Finally, define $h(t) = \prod_{\sigma \in G} (t - \sigma_\alpha(\beta))$. $h(t) \mid q(t)$ so $h(t)$ is the product of some of the irreducible factors of $q(t)$. For each q_k, there is a subset $S_{(k)}$ of S_n such that $q_k(t) = \prod_{\sigma \in S_{(k)}} (t - \sigma_x(\beta))$ and S_n is the disjoint union of the $S_{(k)}$. Since, $(t-\beta) \mid q_1(t)$, $q_1(t) \mid h(t)$.

Theorem: In the above notation, $G_1 = G$.

Proof: (1) $G_1 \subseteq G$ since $q_1(t) \mid h(t)$. (2) $G \subseteq G_1$: If $\rho \in G$, $\rho(q_1(t)) = \prod_{\sigma \in S_1} (t - \rho(\sigma_x(\beta)))$ and $\rho(q_1(t)) = \prod_{\sigma \in S_{(1)}} (t - \rho(\sigma_x(\beta))) = \prod_{\sigma \in S_{(1)}} (t - \rho_\alpha^{-1}(\sigma_x(\beta))) = \rho_\alpha^{-1}(q_1(t))$. So, $\rho \in G_1$.

Theorem: Let R be a UFD and p a prime. Set $\overline{R} = R/(p)$ and let Q_R and $Q_{\overline{R}}$ be their fields of quotients. Let $f(x)$ and $\overline{f(x)}$ be corresponding polynomials with no double roots with corresponding splitting fields K and $\overline{K}$ respectively. Then $\mathcal{G}(\overline{K}/Q_{\overline{R}}) < \mathcal{G}(K/Q_R)$.

Proof:

Definition: A *valuation* is a map $\varphi : K \to \mathbb{F}^{\geq 0}$ where $\mathbb{F}$ is an ordered field such that $\varphi(ab) = \varphi(a)\varphi(b)$, $\varphi(0) = 0$, $\varphi(x) > 0$ if $x \neq 0$ and $\varphi(a+b) \leq \varphi(a) + \varphi(b)$. If $a = \frac{s}{t} p^n$, $\varphi(a) = p^{-n}$ is a valuation. **Ostowski:** A non trivial valuation of $\mathbb{Q}$ is either (i) $\varphi(a) = |a|^\rho, 0 < \rho \leq 1$ (the Archemedean valuation) or (ii) $\varphi(a) = \varphi_p(a)$ (the $p-$adic valuation. $w(a) = log(\varphi(a))$ is the exponential valuation. Set $\wp = \{a : w(a) > 0\}$. Hensel: Let K be complete in the exponential valuation w and $f(x)$ a primitive polynomial in $K[x]$ with integral coefficients. Let g_0, h_0 be polynomials with integral coefficients such that $f(x) = g_0(x)h_0(x)$ $(\wp)$ then there are polynomials $f(x), h(x)$ with integral coefficients in K such that (1) $f(x) = g(x)h(x)$, (2) $g(x) = g_0(x)$ $(\wp)$, (3) $h(x) = h_0(x)$ $(\wp)$ provided $(g_0(x), h_0(x)) = 1$ further $deg(g) = deg(g_0)$ $(\wp)$.

Definition: F is *perfect* iff every irreducible polynomial is separable.

Theorem: F is perfect if (1) $char(F) = 0$, (2) $char(F) = p$ and every element is a pth root, (3) $F = GF(q)$, (4) F is algebraically closed, (5) every finite field is perfect.

Proof of 2: Suppose F^p is not contained in F. Let $a \notin F^p$. $x^p - a$ is irreducible. Since the derivative is 0, this is inseparable. Hence F is not perfect. Suppose $f(x)$ is an inseparable irreducible polynomial in $F[x]$ then $(f, f') \neq 1$. So $f(x) = a_0 + a_p x^p + \ldots + = b_0 + b_p^p x + b_{2p}^p x^{2p} + \ldots)^p$ contrary to irreducibility. Hence $F \neq F^p$.

Definition: Let $E = F[\theta]$ and $\rho = a_0 + a_1\theta + \ldots + a_{n-1}\rho^{n-1}$. $T(\rho) = \sum_{g\in\mathcal{G}(E/F)} \rho^g$ is the *trace* and $N(\rho) = \prod_{g\in\mathcal{G}(E/F)} \rho^g$ is the *norm*; both are in F.

Automorphisms of a finite field: For every $q = p^n$ there is, up to isomorphism, only one field $F = GF(q)$ and the multiplicative group is cyclic. Consider $f(x) = x^h - 1, h = q - 1$ whose roots are roots of 1. The automorphisms of F are exactly $\sigma_i : x \mapsto x^{p^i}$. If $char(F) = p$, every irreducible polynomial $f(x)$ of degree n either has distinct roots or is of the form $\phi(x^p)$ in which case all roots have the same multiplicity p^l for some $l > 0$ with $n = n'p^l$ in which case there are n' relative automorphisms. Thus in successive extensions there are $\prod_i n'_i$ relative automorphisms which have cardinality $[E : F]$ if E is a separable extension and $< [E : F]$ if not.

Theorem: If G is solvable, $G^{(n)} = 1$ for some n. If $n > 4$, $S_n^{(m)}$ contains every 3 cycle for every m.

Proof: $G^{(0)} \supseteq G^{(1)} \supseteq \ldots \supseteq G^{(m)} = 1$ is a composition series with abelian composition factors. This can be refined into a composition series with composition factors of prime order. For the second part, note that $(123) = (13)(12)(13)(12) \in S_n^{(1)}$. Replacing 1 by a, 2 by b and 3 by c shows $(abc) \in S_n^{(1)}, \forall a, b, c$. We show by induction that if H contains all 3-cycles, so does H', if $n \geq 5$. Since $(123)(234) = (13)(24)$, $(ab)(cd) \in H'$. $[(bc)(de), (abc)] = (abc) \in H'$ so any 3-cycle is in H'.

Cyclic Extensions: Suppose $f \in k[x], deg(f) = n$ and let $\mathcal{G}_f(k)$ denote $\mathcal{G}(K/k)$ where K is the splitting field for f over k. Then $\mathcal{G}_f(k)$ is isomorphic to some subgroup of S_n and if f is irreducible, the group is transitive on n symbols. Set $\Delta = \prod_{i<j}(u_i - u_j)$ and $Disc_k(f) = \Delta^2$, then if f is irreducible, the Galois group is A_3 or S_3 according to whether $Disc_k(f) = \Delta^2$ is a square in k. If f is a quartic with separated roots u_1, u_2, u_3, u_4 and $\alpha = u_1u_2 + u_3u_4$, $\beta = u_1u_3 + u_2u_4$, $\gamma = u_1u_4 + u_2u_3$; setting $K = k(\alpha, \beta, \gamma)$ and $[K : k] = m$, then $\mathcal{G}_f(k)$ is S_4 if $m = 6$, $\mathcal{G}_f(k)$ is A_4 if $m = 3$, $\mathcal{G}_f(k)$ is $\mathbb{Z} \times \mathbb{Z}$ if $m = 1$, and $\mathcal{G}_f(k)$ is $\mathbb{Z}_4$ or D_4 if $m = 2$.

Embeddings: Let $k \subset K \subset \overline{k}$ and $\sigma_1, \sigma_2, \ldots, \sigma_r$ be the distinct k-monomorphisms from $K \to \overline{k}$, for $u \in K$, define $N_k^K(u) = (\prod_i \sigma_i(u))^{[K:k]_i}$ and $Tr_k^K(u) = (K : k]_i \sum_i \sigma_i(u)$. Note that distinct automorphisms are linearly independent. From now on, assume all extensions are separable (even Galois). $N_k^K(uv) = N_k^K(u)N_k^K(v)$ and $Tr_k^K(u+v) = Tr_k^K(u)+Tr_k^K(v)$; if $u \in k$, $N_k^K(u) = u^{[K:k]}$ and $Tr_k^K(u) = [K : k]u$; if E is an intermediate field, $N_k^K(u) = N_k^E(N_E^K(u))$ and $Tr_k^K(u) = Tr_k^E(Tr_E^K(u))$. If K is a cyclic extension of k of degree n with generator σ then $Tr_k^K(u) = 0$ iff $\exists v \in K : u = v - \sigma(v)$ and $N_k^K(u) = 1$ iff $\exists v \in K : u = v(\sigma(v))^{-1}$. If $n = mp^t, (p, n) = 1$ where $char(k) = p \neq 0$, there are intermediate cyclic fields, all of which, except the last have degree p and each of which is the splitting field of $f(x) = x^p - x + a$. If $char(k) = p \neq 0$, K is a cyclic extension of degree p iff K is the splitting field of an irreducible polynomial $f(x) = x^p - x - a$ and $K = k(u), f(u) = 0$. Suppose ζ is a primitive nth root of unity over k and $K = k(\zeta)$, if $d \mid n$, $\zeta^{n/d}$ is a primitive d-th root of unity and, K is the splitting field over k of an irreducible polynomial $f(x) = x^d - a, a \in k$. If k contains a primitive n-th root of unity, ζ, TFAE: (1) K is cyclic of degree d $d \mid n$, (2) K is the splitting field over k of $f(x) = x^n - a, a \in k$, (3) K is the splitting field over k of an irreducible polynomial $f(x) = x^d - a, a \in k$.

Satz 90: Let E/F be a cyclic extension with Galois group generated by σ then (a) $N_{E/F}(x) = 1$ iff $\exists y \in E : x = y/\sigma(y)$; and, (b) $T_{E/F}(x) = 0$ iff $\exists y \in E : x = y - \sigma(y)$. Let $(n, char(k)) = 1$, and K a *cyclotomic extension* of k, then, (1) $K = k(\zeta)$ where ζ is a primitive n-th root of unity; (2) K is an *abelian extension* of k of dimension $d, d \mid \psi(n)$; (3) $|\mathcal{G}(K/k)| = d$ and is a subgroup of $\mathbb{Z}_n^*$.

Proof of additive part: If such an α exists then $Tr_k^K(\beta) = 0$ as σ permutes the elements. Conversely, suppose $Tr_k^K(\beta) = 0$, $\exists\theta : Tr_k^K(\theta) \neq 0$. Let $\alpha = \frac{1}{Tr(\theta)}[\beta\theta^\sigma + (\beta + \sigma\beta)\theta^{\sigma^2} + \ldots + (\beta +$

$\sigma\beta + \ldots + \sigma^{n-2}\beta)\theta^{\sigma^{n-1}}]$. From this, we get $\beta = \alpha - \sigma\alpha$.

Proof of multiplicative part: Assume α exists. $N(\beta) = \frac{N(\alpha)}{N(\sigma(\alpha))}$ and since elements of G permute these, $N(\beta) = 1$. Now suppose $\tau, \tau' \in G, \xi \in E : \xi^{\tau+\tau'} = \xi^{\tau}\xi^{\tau'}$. By Artin's theorem on characters, the map given by $id + \beta\sigma + \beta^{1+\sigma}\sigma^2 + \ldots + \beta^{1+\sigma+\ldots+\sigma^{n-2}}\theta^{\sigma^{n-1}} \neq 0$. Hence $\exists\theta \in K : \alpha = \theta + \beta\theta^{\sigma} + \beta^{1+\sigma}\theta^{\sigma^2} + \ldots + \beta^{1+\sigma+\ldots+\sigma^{n-2}}\theta^{\sigma^{n-1}} \neq 0$. $\beta\alpha^{\sigma} = \alpha$ using the fact that $N(\beta) = 1$ and so applying σ to the last term in the sum, we obtain θ. Dividing by α^{σ}, the proof concludes.

Radical extensions: $K = k(u_1, u_2, \ldots, u_n)$ where $\exists n_1 : {u_1}^{n_1} \in k$ and $\exists n_m : {u_m}^{n_m} \in k(u_1, \ldots, u_{m-1})$. f is said to be solvable by radicals if there is a radical extension containing the splitting field of f. If K is a radical extension of k and E is an intermediate field then $\mathcal{G}(E/k)$ is solvable. If E is a finite dimensional extension of degree n, $char(k) \nmid [E : k]$ and $\mathcal{G}(E/k)$ is solvable then there is a radical extension K of k containing E. If $char(k) \nmid n!$ and $f \in k[x], deg(f) = n$ then $f(x) = 0$ is solvable by radicals iff $\mathcal{G}_f$ is solvable. To show this, it suffices to consider prime exponents but we need to prove:

Theorem: If $q \nmid char(F)$ then the q-th root of unity are expressible as radicals, q, a prime.

First a **Lemma:** If $x^p - a$ is reducible, a is a p-th power.

Proof: If $x^p - a = \psi(x)\phi(x)$, each is a product of factors of the form $(x - \zeta_\nu\theta)$ where ζ is a p-th root of unity and $\theta^p = a$. Say, $\psi(x) = b_k x^k + \ldots + b_0$ is a product of k of them. $(p, k) = 1$ so $cp + dk = 1$ for some $c, d \in \mathbb{Z}$. Further, $b = b_0 = \zeta^\nu\theta^k$. So $a = a^{cp} \cdot a^{dk} = b^{dp} \cdot a^{cp}$ which proves the result.

Proof of Theorem: By induction on q, clear for $q = 2$. The q-th roots of unity form a cyclic extension of degree $q - 1 = p_1^{e_1} \ldots p_k^{e_k}$. By induction, the successive p_i-th roots of unity are radicals and adjoining them, $x^{p_k} - a$ must be irreducible by the lemma so each such extension is a radical extension.

Theorem: Let R_m be the ring of integers in $\mathbb{Q}[\sqrt{m}]$. Suppose $\forall x, y \in R_m$, with $y \nmid x$ and $|N(x)| \geq |N(y)|$, $\exists u, v \in R_m$ such that $N(xu - yv) \leq |N(y)|$. Then R_m is a PID.

Proof: Let I be an ideal and assume, by way of contradiction, R_m is Euclidean. Choose $y \neq 0$ so that $|N(y)|$ is minimal. WTS $y \mid x$. We can find u, v: $N(xu - yv) \leq |N(y)|$ but this contradicts the minimality of $|N(y)|$. Thus $y \mid x$ and $I = (y)$.

Theorem: R_{-19} is a PID.

Proof: $R_{-19} = \frac{a+b\sqrt{m}}{2}$. Suppose $y \nmid x$, $|N(x)| \geq |N(y)|$. $\frac{x}{y} = \frac{a+b\sqrt{m}}{c}, c > 1$. Each of the cases $c = 2, c = 3, c = 4, c \geq 5$, yield contradictions.

Theorem: If $m \in \mathbb{Z}^{<0}$ is square-free and $m \notin \{-1, -2, -3, -7, -11\}$, then R_m is not a Euclidean domain.

Proof: Suppose if is. CHoose $b \in R_m \setminus U(R_m)$ with $d(b)$ minimal. $\forall a, a = bq + r$ and $r = 0, \pm 1$, so $b \mid 2, 3$. However, both 2 and 3 are irreducible in R_m. If $m = 1 \pmod 4$ and put $a = \frac{1+\sqrt{m}}{2}$. Neither $a, a + 1, a - 1$ are divisible by 2 or 3. Contradiction.

Theorem: R_{-19} is a PID that is not a Euclidean domain.

Proof: By the above, R_{-19} is not a Euclidean domain and is a PID.

1.2.7 Computational Algebra

Discrete Fourier Transform and FFT: Let $c(x) = a(x)b(x)$ which corresponds to the convolution $\vec{c} = \vec{a} * \vec{b}$. Define the DFT as $F(\vec{a}) = A\vec{a}$, $A = \omega^{ij}$ with inverse $A^{-1} = \frac{1}{n}\omega^{-ij}$. Note that $F(\vec{b} * \vec{c}) = F(\vec{b}) \cdot F(\vec{c})$ (pointwise multiplication). *Tukey-Cooley Idea:* Suppose $n = pq$, set $j = j(j_1, j_2) = j_1 q + j_2, k = k(k_1, k_2) = k_2 p + k_1, 0 \leq j_1 < p, 0 \leq j_2 < q, 0 \leq k_1 < p, 0 \leq k_2 < q$. Then $\hat{f}(k_1, k_2) = \sum_{j_2=0}^{q-1} e^{\frac{2\pi i j_2 (k_2 p + k_1)}{n}} \sum_{j_1=0}^{p-1} e^{\frac{2\pi i j_1 k_1}{p}} f(j_1, j_2)$. This requires $p^2 q$ and $q^2 p$ operations respectively or $pq(p+q)$ rather than $(pq)^2$. Now do this recursively if p, q factor further. $X_n = \sum_{k=0}^{N-1} x_k e^{-ikn}$. $x_n = \frac{1}{N} \sum_{k=0}^{N-1} X_k e^{ikn}$.

Strassen and FFT: For matrix multiply, Strassen found 7 products that do the trick. $m_1 = (a_{12} - a_{22})(b_{21} - b_{22})$, $m_2 = (a_{11} + a_{22})(b_{11} + b_{22})$, $m_3 = (a_{11} - a_{21})(b_{11} + b_{12})$, $m_4 = (a_{11} + a_{12})b_{22}$, $m_5 = a_{11}(b_{21} - b_{22})$, $m_6 = a_{22}(b_{21} + b_{11})$, $m_7 = (a_{21} + a_{22})b_{11}$. $c_{11} = m_1 + m_2 - m_4 + m_6$, $c_{12} = m_4 + m_5$, $c_{21} = m_6 + m_7$, $c_{22} = m_2 - m_3 + m_5 - m_7$. $T(n) = 7T(\frac{n}{2}) + 18\frac{n}{2}^2$, which is $O(2^{lg(7)})$. $F_{i,j} = \omega^{ij}$. F evaluates, F^{-1}, interpolates. $q_{l,m} = \prod_{j=l}^{l+2^m-1}(x - c_j)$ and $q_{l,m} = a_{l,m-1} q_{l+2^m, m-1}$. What is $Rem(\frac{p(x)}{q_{l,0}(x)}), \forall l$? If $q = q'q''$, $Rem(\frac{p(x)}{q'(x)}) = Rem(\frac{r_{l,m}(x)}{q'(x)})$, $q_{l,m} = x^{2^m} = \omega^{rev(l/2^m)}$. For algorithm, crucial step is $r_{l,m}(x) = \sum(a_j + \omega^s a_{j+2^m})x^j$ and $r_{l+2^m,m}(x) = \sum(a_j + \omega^{s+\frac{n}{2}} a_{j+2^m})x^j$.

Hensel: If $I \subseteq \mathbb{R}$, $f = gh \pmod I$ such that the pseudo $GCD(g, h) = 1$ then $\exists g^*, h^*$ such that (1) $f = g^* h^* \pmod{I^2}$, (2) $g = g^* \pmod I$, (3) $h = h^* \pmod I$, and pseudo $GCD(g^*, h^*) = 1 \pmod{I^2}$. If g', h' satisfy the conditions also, $g' = g^*(1 + u) \pmod{i^2}$ and $h' = h^*(1 - u) \pmod{i^2}$.

Bivariate Factoring: If $|\mathbb{F}| > 4d^2$, $f \in \mathbb{F}$, $deg_x(f) \leq d$, $\exists \in \mathbb{F}$: $f_\beta(x, 0) \in \mathbb{F}[x]$ has no repeated factors.

1a Obtain square free factorization.
1b Find $\beta \in \mathbb{F}$ such that $f(x, \beta)$ is squarefree.
1c $f_\beta = f(x, y + \beta)$.
2a $f(x, y) = g(x, y)h(x, y) \pmod y$.
2b Lift $f(x, y) = g_k(x, y)h_k(x, y) \pmod{y^k}$.
3a Find g'' and l_k: $g'' = g_k l_k \pmod{y^{2^k}}$, $deg_x(g'') \leq deg_x(f)$, $deg_y(g'') \leq deg_y(f)$, $g'' \neq 0$.
$|Res(f, g, x)| \leq (m+1)^{\frac{n}{2}} (n+1)^{\frac{m}{2}} A^{\frac{m}{2}} B^{\frac{n}{2}}$.

Extension Theorem: Let $I = \langle f_1, ..., f_s \rangle \in \mathbb{C}(x_1, x_2, ..., x_n)$ and I_1 is the first elimination ideal of I. For each $1 \leq i \leq s$ write $f_i = g(x_2, ..., x_n){x_1}^{N_i} + ...$ Suppose $c = (c_2, ..., c_n) \in V(I_1)$. If $c \notin V(g_1, g_2, ..., g_s)$, $\exists c_1$ such that $(c_1, c) \in V(I)$.

Linear Programming: $max(cx)$ subject to $Ax \leq b, x \geq 0$. **Quadratic Programming:** $max(\sum \rho_{ij} \sigma_i \sigma_j x_i x_j)$, subject to $\sum x_i = 1$, $x_i \geq 0$, $\sum x_i u_i \geq R$.

1.2.8 Algebraic Number Theory

Gaussian Integers: $\mathbb{Z}[i]$. Let $\alpha, \beta, \gamma, \delta$ represent gaussian integers. $N(x + yi) = x^2 + y^2$. $\forall \alpha, \beta, \exists \gamma, \delta$ such that $\alpha = \beta\gamma + \delta$ with $0 \leq N(\delta) < N(\beta)$. α is a unit iff $N(\alpha) = 1$. Units are $1, -1, i, -i$. Let $S = \{\alpha\eta + \beta\gamma\}$, ϕ with minimal norm is the gcd. If π is a Gaussian integer with $N(\pi) = p$ then π is prime. If π is a Gaussian prime and $\pi | \alpha\beta$ then $\pi | \alpha$ or $\pi | \beta$. Gaussian integers form a UFD. Let π be a Gaussian prime, there is one and only one p such that $\pi | p$. Note that $\pi = x + yi$, $N(\pi) = x^2 + y^2$ divides p or p^2 so $x = 0, 1, 2 \pmod 4$. Characterization of Gaussian primes: $p = 2$: $p = -i\pi^2$. $p = 3 \pmod 4$, $p = \pi$. $p = 1 \pmod 4$, $p = \pi\overline{\pi}$ and π and $\overline{\pi}$ are non-associated primes. If $p = 1 \pmod 4$ then $p \mid (z^2 + 1)$. If $\pi \mid p$, $\pi | (z + i)(z - i)$ so $\pi | (z - i)$.

Definitions: x is *integral* over A if x is a root of a monic polynomial f with coefficients in A. If A is a subring of R, the *integral closure* of A in R is the set A_c of elements of R that are integral over A. Note that $A \subseteq A_c$. We say A is integrally closed in R if $A_c = A$. If A is an integral domain with quotient field K, and A is integrally closed in K we simply say that A is integrally closed without reference to R.

Theorem: Let M be an A-module. M is faithful if $aM = 0 \rightarrow a = 0$. Let $A \subseteq B$, $\alpha \in B$. The following are equivalent: (1) α is a root of $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_0$; (2) $A[\alpha]$ is a finitely generated A module; (3) $\exists$ a faithful module, N, over $A[\alpha]$ which is a finitely generated A-module.

Proof: $1 \rightarrow 2$: $1, x, \ldots, x^{n-1}$ generate $A[x]$. $2 \rightarrow 3$: $N = A[x]$. $3 \rightarrow 1$: Let $\beta_1, \ldots, \beta_n$ be the generators of N. $x\beta_i = \sum_j a_{ij}\beta_j$ and $det(xI - (a_{ij})) = 0$. This gives the monic equation.

More trace and norm: $N_{E/F}(x) = det(m(x))$, $Tr_{E/F}(x) = trace(m(x))$. If $\alpha = x + yi$, $Tr(\alpha) = 2x$, $N(\alpha) = \alpha\overline{\alpha}$. $S(\alpha) = \sum_\sigma \alpha^\sigma$ is an integer, so is $N(\alpha) = \prod_\sigma \alpha^\sigma$. α is a unit iff $|N(\alpha)| = 1$. α is an integer of $Q(\sqrt{d})$ iff $T(\alpha)$ and $N(\alpha)$ are integers.

Quadratic integers: $I_d = \{x + y\omega_d, x, y \in \mathbb{Z}\}$, $\omega_d = \sqrt{d}$ if $d = 2, 3 \pmod 4$, $\frac{1+\sqrt{d}}{2}$, if $d = 1 \pmod 4$. Ideal Theory: $P = (2, 1 + \sqrt{-5})$, $Q = (3, 1 + \sqrt{-5})$. $P^2 = (2)$ and $Q\overline{Q} = (3)$. Fermat analogue: $\alpha^{N(\pi)-1} = 1 \pmod \pi$.

Theorem: If θ is an algebraic number, there is an integer m such that $m\theta$ is an algebraic integer.

Proof: We may assume $a_n\theta^n + a_{n-1}\theta^{n-1} + \ldots + a_0 = 0, a_i \in \mathbb{Z}$. Then $(a_n\theta)^n + a_{n-1}(a_n\theta)^{n-1} + \ldots + (a_n)^{n-1}a_0 = 0$. $a_n\theta$ is an algebraic integer.

Notation: $R(\theta)$ denotes the ring of algebraic integers in $\mathbb{Q}(\theta)$.

Theorem: Every basis for $R(\theta)$ has n elements, where θ is an algebraic number whose minimal polynomial has degree n.

Proof: Every integral basis is a basis and has the same number of elements.

Definition: $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = det({\alpha_i}^{\sigma_j})^2$, $\alpha_i \in R(\theta)$. Alternatively, $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = det(T(\alpha_i\alpha_j))$; this follows from the fact that $T(\alpha_i\alpha_j) = \sum_k \sigma_k(\alpha_i\alpha_j)$.

Theorem: $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is an integer.

Proof: $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is an algebraic integer fixed by all $\sigma \in \mathcal{G}(\mathbb{Q}(\theta)/\mathbb{Q}$ and so it is in $\mathbb{Q}$. The only algebraic integers in $\mathbb{Q}$ are in $\mathbb{Z}$.

Theorem: If $\{\alpha_i\}$ and $\{\beta_i\}$ are basis with $\alpha_j = \sum_k a_{jk}\beta_k$ then $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = det(a_{ij})^2\Delta(\beta_1, \beta_2, \ldots, \beta_n)$.

Proof: $T(\beta_r\beta_s) = T(\sum_{i,j} a_{r,i}a_{s,j}\alpha_i\alpha_j$, so $(T(\beta_r\beta_s)) = (a_{ij})T(\alpha_i\alpha_j)(a_{ij})^T$. Taking determinants gives the result.

Theorem: Suppose F is separable over $\mathbb{Q}$, $\langle\alpha_i\rangle$ is a basis iff $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) \neq 0$.

Proof: If $\sum_j c_j\alpha_j = 0$, $\sum_j c_j\sigma_k(\alpha_j) = 0, \forall k$ and $B = (\sigma_i(\alpha_j))$ has linearly dependent columns so the determinant (discriminant) is 0. Suppose $\langle\alpha_1, \ldots, \alpha_n\rangle$ are a basis and $\exists c_j$ not all 0 such that $\sum_j c_j\sigma_k(\alpha_j) = 0$. If $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = 0$, the rows of B are linearly dependent so $\sum_j c_j\sigma_k(u) = 0, \forall u$, which contradicts Artin.

Theorem: All integral bases of $R(\theta)$ have the same discriminant.

Proof: If $\langle \alpha_1, \ldots, \alpha_n \rangle$ and $\langle \beta_1, \ldots, \beta_n \rangle$ are two bases $\alpha_j = \sum_k a_{jk}\beta_k$ and $\beta_j = \sum_k b_{jk}\alpha_k$. $det(a_{ij})^2 = det(b_{ij})^2 = 1$.

Definition: If $\{\alpha_i\}$ is an integral basis for $R(\theta)$ then $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is minimal, in which case it is called the *discriminant* of $R(\theta)$ and written $Disc(R(\theta))$.

Theorem: If A is an ideal of $R(\theta)$ then $\mathbb{Z} \cap A \neq \emptyset$.

Proof: Since A is an ideal, $R(\theta)A \subseteq A$. If $\alpha \in A$, $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 = 0, a_i \in \mathbb{Z}$. $a_0 \in \mathbb{Z} \cap A$.

Theorem: If D is a ring of algebraic integers and A is a module then D/A is finite.

Proof: $\exists a \in A \cap \mathbb{Z}$. $(a) \subseteq A$ so $D/(a) \to D/A$ is a homomorphism. $D = \mathbb{Z}\omega_1 + \ldots + \mathbb{Z}\omega_n$. Let $S = \{\sum_i \gamma_i\omega_i, 0 \leq \gamma_i < a\}$. S contains all coset representatives of $D/(a)$.

Theorem: D is Noetherian.

Proof: Since D/A_i is finite there are only finitely many ideals in A_1.

Theorem: Every prime ideal in D is maximal.

Proof: D/P is a finite integral domain.

Theorem: Let $A \subseteq D$ be an ideal. If $\beta \in F$ and $\beta A \subseteq A$ then $\beta \in D$.

Proof: A is a finitely generated $\mathbb{Z}$-module. β satisfies $a_n B^n + \ldots + a_0 = 0, a_i \in \mathbb{Z}$. Multiply by a_n^{n-1} and $a_n\beta$ is an algebraic integer. $a_i a_n^{-1} \in \mathbb{Z}$.

Theorem: If A, B are ideals in D and $A = AB$ then $B = D$.

Proof: Let $\alpha_1, \ldots, \alpha_n$ be an integral basis for A. $\exists b_i \in B : \alpha_i = \sum_j b_{ij}\alpha_j$. $det(b_{ij} - \delta_{ij}) = 0$. So $1 \in B$ and $D = B$.

Theorem: If $\omega \in D$ and $(\omega)A = BA$ then $(\omega) = B$.

Proof: $\beta \in B$ implies $(\beta/\omega)A \subseteq A$ so $\beta/\omega \in D$. $A = \omega^{-1}BA$ so $\omega^{-1}B = D$.

Theorem: Every ideal contains a basis.

Proof: Let $\beta_1, \ldots, \beta_n$ be a basis of $F/\mathbb{Q}$. $\exists a, b \in \mathbb{Z}$ such that $b\beta_1, \ldots, b\beta_n \in \mathbb{Z}$. Choose $\alpha \in A, \alpha \neq 0$, $b\beta_1\alpha, \ldots, b\beta_n\alpha \in A$ are a basis.

Theorem: $\exists M(F) : \alpha, \beta \in D, \beta \neq 0, 1 \leq t \leq M$ and $\omega \in D$: $|N(t\alpha - \omega\beta)| < |N(\beta)|$.

Proof: Let $\gamma = \frac{\alpha}{\beta} \in F$. It suffices to show that $\forall \gamma \in F$, there is an $M : |N(t\alpha - \omega\beta)| < 1$ for some $1 \leq t \leq M$ and $\omega \in D$. Let $\omega_1, \ldots, \omega_n$ be an integral basis for D. For $\gamma \in F$, $\gamma = \sum_{i=1}^n \gamma_i\omega_i, \gamma_i \in \mathbb{Q}$. Notice that $|N(\gamma)| = |\prod_j (\sum_i \gamma_i\omega_i^{(j)})| \leq C(max_i|\gamma_i|)^n$, where $C = \prod_j (\sum_i \omega_i^{(j)})$. Choose $m > C^{\frac{1}{n}}$ and set $M = m^n$. For $\gamma \in F, \gamma = \sum_i \gamma_i\omega_i$, $\gamma_i = a_i + b_i, a_i = \lceil \gamma_i \rceil$. Put $[\gamma_i] = \sum_i a_i\omega_i$. Map $F \to \mathbb{R}^n$ by $\phi(\sum_i \gamma_i\omega_i) = (\gamma_1, \ldots, \gamma_n)$. Partition the n-cube into $M = m^n$ subcubes. Consider the points $\phi(\{k\gamma\}), 1 \leq k \leq m^n + 1$. At least two lie in the same subcube. Subtracting we get $t\gamma = \omega + \delta$. The coordinates of δ have absolute value $\leq \frac{1}{m}$. So $N(\delta) \leq C(1/m)^n = C/m^n < 1$.

Theorem: The class number is finite.

Proof: Let $A \subseteq D$. For $\alpha \in A$ and $\alpha \neq 0$, $|N(\alpha)| \in \mathbb{Z}$. Choose $\beta \in A, \beta \neq 0 : |N(A)|$ is minimal. $\forall \alpha, \exists t : |N(t\alpha - \omega\beta)| < |N(\beta)|, 1 \leq t \leq M$. Since $t\alpha - \omega\beta \in A$, $t\alpha - \omega\beta = 0$. $B = \frac{1}{\beta}M!A \subseteq D$, $(M!) \supseteq (\beta)B$ so $(M!) \subseteq B$. But $(M!)$ is contained in only finitely many ideals. So $A \equiv B$, where B is one of finitely many ideals.

Theorem: If A, B are ideals in $R(\theta)$, $A|B$ iff $A = BC$ iff $B \subseteq A$.

Proof: $\exists k : B^k = (\beta)$. Since $A \subseteq B$, $B^{k-1}A \subseteq (\beta)$ so $C = \frac{1}{\beta}B^{k-1}A \subseteq D$. $BC = 1$.

Definition: If A is an ideal with basis $\alpha_i = \sum_j a_{ij}\omega_j$ then $N(A) = det(a_{ij})$. $A \sim B$ iff $\exists \alpha, \beta$ such that $(\alpha)A = (\beta)B$. each equivalence class is called an ideal class.

Theorem: $\forall A \subseteq D, \exists k : 1 \leq k \leq h_F$ such that A^k is principal.

Proof: Consider $\{a^i : 1 \leq k \leq h_F + 1\} : a^i \equiv A^j, j > i$. $\exists \alpha, \beta \in D : (\alpha)A^i = (\beta)A^j$. Put $B = A^{j-i}$. B is principal since $(\alpha)A^i = (\beta)BA^i$. $(\alpha/\beta)A^i \subseteq A^i$, so $\omega = \alpha/\beta \in D$ then $(\omega)A^i = BA^i$ and thus $(\omega) = B$.

Theorem: There are finitely many ideal classes h of $R(\theta)$ and $A^h \sim (1)$.

Proof: For $K = R(\theta)$, $\exists C(K) : \forall A, \exists 0 \neq \alpha \in A : |N(\alpha)| \leq CN(A)$. Use this to show $\exists B : N(B) \leq C$ so there are a finite number of ideals containing B. $\exists \alpha : (\alpha) = AD$. $AN \sim AD$.

Theorem: If A is an ideal in $R(\theta)$, $\exists B$ such that $AB = (a)$ for some a in $R(\theta)$.

Proof: Todo.

Theorem: If A, B are ideals in $R(\theta)$,with $AC = BC$ then $A = B$.

Proof: $\exists k > 0 : A^k = (\alpha)$, so $A^{k-1}AB = A^{k-1}AC$. $(\alpha)B = (\alpha)C$ and so $B = C$.

Theorem: If $P|AB$ and P does not divide A then $P|B$.

Proof: $a \in A, b \in B$ $P \supseteq AB$ but $P \not\supseteq A$, so $ab \in P$. $\exists c : ac \in 1 + P$. $ac - 1 \in P$ and $abc - b \in P$ but $ab \in P$ so $b \in P$ and $P \supseteq B$.

Theorem: Every ideal has finitely many distinct divisors.

Proof: Todo.

Theorem: Every prime ideal must divide the principal ideal of a rational prime.

Proof: Follows from finiteness of class number.

Theorem: Every ideal can be written as a product of prime ideals. The factorization is unique apart from order.

Proof: Let A be an ideal. D/A is finite so $A \subset P_1$, maximal and $A = P_1B_1$. If $B_1 \neq D$, B_1 is contained in a maximal ideal and so on giving a chain, $A \subset B_1 \subset B_2 \subset \ldots$ which must terminate.

Theorem: Every rational integer belongs to finitely many ideals.

Proof: Todo.

Theorem: Rational prime is *ramified* if its principal ideal factors into prime ideals in which one prime ideal is repeated. If this happens, $p|\Delta(\alpha_1, \ldots, \alpha_n)$.

Proof: Todo.

Theorem: The ring of integers $\mathcal{D}_K$ in the number field, K, has the following properties: $\mathcal{D}_K$ is a domain with field of fractions K. $\mathcal{D}_K$ is noetherian (Use the fact that $\mathcal{D}_K$ is a free abelian group of degree $n = K : \mathbb{Q}$.)

Proof: Todo.

Definition: Let $\mathcal{D}$ be a ring of integers, $\mathfrak{a}$ is a fractional ideal if $\exists c \in \mathcal{D}$: $c\mathfrak{a} \subseteq \mathcal{D}$.

Theorem: Every non zero prime ideal $\mathfrak{p}$ of $\mathcal{D}$ is maximal. ($\mathcal{D}/\mathfrak{a}$ is a finite integral domain.) Fractional ideals form an abelian group.

Proof: Todo.

Theorem: Every non-zero ideal of $\mathcal{D}$ can be factored into prime ideals ($\mathcal{D}$ is noetherian).

Proof: Todo.

Norm of an ideal: $N(\mathfrak{a}) = |\mathfrak{D}/\mathfrak{a}|$; if $\mathfrak{a} = \langle a \rangle$ is principal $N(a) = N(\mathfrak{a})$. $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$. $\Delta_{K/\mathbb{Q}}(\alpha_1, \alpha_2, \ldots, \alpha_n) = [det(\sigma_i(\alpha_j))]^2$.

Theorem: Every non-zero ideal of $\mathcal{D}$ has a finite number of divisors.

Proof: Todo.

Theorem: A non-zero rational integer belongs to a finite number of ideals of $\mathcal{D}$.

Proof: Todo.

Theorem: Only a finite number of ideals of $\mathcal{D}$ have a given norm.

Proof: Todo.

Theorem: If $\mathfrak{a} \neq \mathfrak{b}$ are ideals of $\mathcal{D}$ then $\exists \alpha \in \mathfrak{a} : \alpha\mathfrak{a}^{-1} + \mathfrak{b} = \mathcal{D}$.

Proof: Todo.

Theorem: Let $\mathfrak{a} \neq 0$ be an ideal of $\mathcal{D}$ and $0 \neq \beta \in \mathfrak{a}, \exists \alpha \in \mathfrak{a} : \mathfrak{a} = \langle \alpha, \beta \rangle$.

Proof: Todo.

Minkowski: X is convex if $x, y \in X \rightarrow \lambda x + (1-\lambda)y \in X, \forall \lambda \in [0,1]$. X is symmetric if $x \in X \rightarrow -x \in X$. Let L be an n-dimensional lattice in $\mathbb{R}^n$ with fundamental region T and let X be a bounded, convex, symmetric subset of $\mathbb{R}^n$; if $v(X) > 2^n v(T), \exists \alpha \in X \cap L, x \neq 0$. Let L be a lattice then $\mathbb{R}^n/L \cong T^n$ (a torus). Let T be a fundamental region of L, $\phi : T \rightarrow T^n$ then $v(X) = v(\phi^{-1}(X))$. If $\nu : \mathbb{R}^n \rightarrow T^n$ is the natural homomorphism with $ker(\nu) = L$. If X is a bounded subset of $\mathbb{R}^n$, ν exists and $v(\nu(X)) \neq v(X)$ then $\nu_{|X}$ is not injective. *Four squares:* If $p = 4k+1$ then $p = a^2 + b^2$. ($\langle g \rangle = \mathbb{Z}_p$ is cyclic $g^k = u$ and $u^2 = -1$. Let $L = \{(a,b) : b = ua \pmod{p}\}$, $\mathbb{Z}^2 : L = p^2$, $vol(T_L) = p$. $C_r : \{x : ||x|| < r\}$ and $\pi r^2 > 4p$, $r^2 = \frac{3p}{2}, 0 \neq a^2 + b^2 \leq r^2 < 2p$.

Examples in algebraic fields: In $R = \mathbb{Z}[\sqrt{-3}]$, $\frac{-1+\sqrt{-3}}{2}$ is a unit note that $2 \times 2 = -1 + \sqrt{-3} \times -1 - \sqrt{-3}$. In $R = \mathbb{Z}[\sqrt{-5}]$ ideals are not all principal; note that $2 \times 3 = -1 + \sqrt{-5} \times -1 - \sqrt{-5}$. *Pell related:* There

are two equivalence classes of forms of determinant 5: x^2+5y^2 and $2x^2+2xy+3y^2$ and the class number of $\mathbb{Z}[\sqrt{-5}]$ is 2. If p is a rational prime and $K/\mathbb{Q}$ is a Galois extension then $G=\mathcal{G}(K/\mathbb{Q})$ acts transitively on the ideal divisors of (p), the exponent of the ideal divisors are called the ramification index. The ideal generated by a rational ideal (p) factors into indecomposable factors in an algebraic number field, O_F, in one of three ways: (a) (p), (b) $(p)=P\sigma(P)$ ("p splits"), or (c) $(p)=P^2$ ("p ramifies").

Analytic formulas: $f*g(n)=\sum_{d|n} f(d)g(\frac{n}{d})$. This is commutative, associative and has an inverse. $\Lambda(n)=ln(n)$, if $n=p^m$, $\Lambda(n)=0$, otherwise. Note: $ln(n)=\sum_{d|n}\Lambda(d)$. $\sigma_\alpha(n)=\sum_{d|n} d^\alpha$. $\psi(x)=\sum_{n\leq x}\Lambda(n)$, $\vartheta(x)=\sum_{p\leq x} ln(p)$. $\frac{\psi(x)}{x}-\frac{\vartheta(x)}{x}\leq\frac{ln(x)^2}{2\sqrt{x}ln(2)}$. $L(1,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n}$, χ, a non-principal character. **Dirichlet:** If $k>0$ and $(h,k)=1$, $\forall x>1$ $\sum_{p\leq x, p=h \pmod k}\frac{ln(p)}{p}=\frac{1}{\phi(k)}ln(x)+O(1)$. $\pi_a(x)=\sum_{p\leq x, p=a \pmod k} 1$. $\pi_a(x)\approx\frac{\pi(x)}{\phi(k)}$, $x\to 0$, $\forall a$, $(a,k)=1$ and $\pi_a(x)\approx\pi_b(x)$ when $(a,k)=(b,k)=1$.

Definition: A *Lie algebra* is a vector space, V over a field, F with an operation $[,]:V\times V\to V$ which is alternating and bilinear and which satisfies the Jacobi identity: $[x,[y,z]]+[y,[z,x]]+[z,[x,y]]=0$. If A is an associative algebra, there is a corresponding Lie algebra with $[a,b]=a*b-b*a$, called an *enveloping algebra. Example:* $n\times n$ matricies over F give rise to $L_n(F)$. $\mathbb{R}^3$ with $[a,b]=a\times b$ is a Lie algebra.

1.3 Analysis, Geometry and Topology

1.3.1 Geometry and Topology

$[\vec{a},\vec{b},\vec{c}] = \vec{a}\cdot(\vec{b}\times\vec{c})$. Plane Π, perpendicular to unit vector $\vec{n}$ and containing $\vec{a}$: $\vec{x}\cdot\vec{n} = \vec{a}\cdot\vec{n} = d$. Distance from $\vec{y}$ to Π is $|d-\vec{y}\cdot\vec{n}|$. $\vec{x}\times\vec{y} = (x_2y_3-y_2x_3)\vec{i}+(x_3y_1-y_3x_1)\vec{j}+(x_1y_2-y_1x_2)\vec{k}$. Denote $[\vec{a},\vec{b}]$ as the line from $\vec{a}$ to $\vec{b}$; $[\vec{x_0},\vec{x_0}+\vec{a}] = \{\vec{x} : (\vec{x}-\vec{x_0})\times\vec{a} = 0\}$. So the line that includes $\vec{x_0}$ and $\vec{x_1}$ is $\{\vec{x} : (\vec{x}-\vec{x_0})\times(\vec{x_1}-\vec{x_0}) = 0\}$. Denote $[\vec{a},\vec{b},\vec{c}]$ as the plane containing $\vec{a}$, $\vec{b}$ and $\vec{c}$. $\vec{a}\times(\vec{b}\times\vec{c}) = (\vec{a}\cdot\vec{c})\vec{b}-(\vec{a}\cdot\vec{b})\vec{c}$. Let θ be the angle (measured counterclockwise) between $[0,u]$ and $[0,v]$ then $\Delta(u,v) = u_1v_2-u_2v_1 = |u||v|sin(\theta)$. $\Delta(u,v,w) = [u,v,w] = det\begin{pmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{pmatrix}$. Distance between $(\vec{x}-\vec{x_0})\times\vec{a} = 0$ and $(\vec{x}-\vec{x_1})\times\vec{b} = 0$ is $\frac{(\vec{x_0}-\vec{x_1})\cdot(\vec{a}-\vec{b})}{||\vec{a}\times\vec{b}||}$. Rotation through θ: $x' = xcos(\theta)+ysin(\theta)$, $y' = ycos(\theta)-xsin(\theta)$.

Moebius Transformations: $\mathbb{C}_\infty = \mathbb{C}\cup\{\infty\}$. $\mathcal{M} = \{\tau_{a,b,c,d}(z) : \tau_{a,b,c,d}(z) = \frac{az+b}{cz+d}\}$. If $\tau_{a,b,c,d}(z) = \tau_{\alpha,\beta,\gamma,\delta}(z)$, $\exists\lambda\in\mathbb{C}$ such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \lambda\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. If $\tau\in\mathcal{M}$, $\tau:\mathbb{C}_\infty\to\mathbb{C}_\infty$ and τ is a product of maps of the following type: $z\mapsto az$, $z\mapsto z+b$ and $z\mapsto\frac{1}{z}$. For all ordered points, $\langle z_1,z_2,z_3\rangle, \langle w_1,w_2,w_3\rangle$ in $\mathbb{C}_\infty$, there is a unique $\tau\in\mathcal{M}$ such that $\tau(z_i) = w_i$. For ordered points, $\langle z_1,z_2,z_3,z_4\rangle, \langle w_1,w_2,w_3,w_4\rangle$ in $\mathbb{C}_\infty$, there is a $\tau\in\mathcal{M}$ such that $\tau(z_i) = w_i$ iff the cross-ratio of $[z_1,z_2,z_3,z_4]$ equals the cross ratio of $[w_1,w_2,w_3,w_4]$. $\Phi : GL_2(\mathbb{C})\to\mathcal{M}$ is a surjective homomorphism given by $\Phi(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \frac{az+b}{cz+d}$; the kernel of the homomorphism is $\lambda I, \lambda\in\mathbb{C}$. The restriction of Φ to $SL_2(\mathbb{C})$ is also a surjection with kernel $\pm I$. The *modular group* SL_2 is the subset of $\mathcal{M}$ with $ad-bc = 1$ with the obvious identification and is generated by $\tau\mapsto\tau+1, \tau\mapsto-\frac{1}{\tau}$. Note fundamental region. Set $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$; these correspond to $S(z) = \frac{-1}{z}$ and $T(z) = z+1$. Define $H = \{z : Im(z) > 0\}$ and $D = \{z : -\frac{1}{2}\le Re(z)\le 0, |z| = 1\vee -\frac{1}{2}\le Re(z) < \frac{1}{2}, |z| > 1\}$. $\mathcal{M}$ maps H into itself and D is a fundamental domain for SL_2.

Spherical triangles: $cos(a) = sin(b)sin(c)cos(A)+cos(b)cos(c)$, $\frac{sin(a)}{sin(A)} = \frac{sin(b)}{sin(B)}$.

Some identities: $cos(Y)-cos(X) = 2sin(\frac{X+Y}{2})sin(\frac{X-Y}{2})$. $cos(Y)+cos(X) = 2cos(\frac{X+Y}{2})cos(\frac{X-Y}{2})$. $sin(Y)+sin(X) = 2sin(\frac{X+Y}{2})cos(\frac{X-Y}{2})$. $sin(X)-sin(Y) = 2cos(\frac{X+Y}{2})sin(\frac{X-Y}{2})$.

Definition: The *circumcenter* is the common intersection of the 3 perpendicular bisectors of each side of a triangle. The *incenter* is the common intersection of the 3 angle bisectors of each side of a triangle. The *orthocenter* is the intersection of the altitudes. Angle bisector divides opposite side in proportion to adjacent sides. The *centroid* is the intersection of the medians.

Theorems: A triangle is divided into six triangles of equal area by the medians. The medians of a triangle divide one another in the ratio 2 : 1. The orthocenter, centroid, and circumcenter are collinear. The centroid divides the distance from the orthocenter to the circumcenter by the ration of 2 : 1.

> *Proof:* The medians are concurrent by Ceva's theorem below. In triangle ABC, numbering the sub-trangles I, II, III, IV, V, VI starting from A and going clockwise. $\mathcal{A}(I) = \mathcal{A}(II)$, $\mathcal{A}(III) = \mathcal{A}(IV)$, and $\mathcal{A}(V) = \mathcal{A}(VI)$. Also, $\mathcal{A}(I)+\mathcal{A}(II)+\mathcal{A}(III) = \mathcal{A}(IV)+\mathcal{A}(V)+\mathcal{A}(VI)$, so $\mathcal{A}(I) = \mathcal{A}(VI)$. A similar argument shows $\mathcal{A}(I) = \mathcal{A}(III)$.

Theorems: In triangle ABC, (1) let O be the circumcenter, then $OA = OB = OC$; (2) let P be the incenter, the $d(AB, P) = d(BC, P) = d(AC, P)$.

Proof: Again, the altitudes are concurrent by Ceva. Draw the diagram and use Pythagoras and similar triangles.

Pick's Theorem: Let B be a polygon which contains n_i interior lattice points and n_b lattice points on its boundary. $A(B) = n_i + \frac{n_b - 2}{2}$.

Proof: The theorem is true for all right triangles with no interior points in the lattice. If the theorem is true for a polygon P and T is a triangle with a single point not in T, the theorem holds for $T \cup P$.

Two theorems on triangles: In triangle ABC, suppose D lies on BC, $BD = p$, $CD = q$, then $AD^2 = \frac{pb^2 - qc^2}{p+q} - pq$. In triangle, ABC suppose the angle bisector of A meets BC at D, $BD = p$ and $CD = q$, then $\frac{p}{c} = \frac{q}{b}$.

Definition: A *flex* is a non-singular point intersecting P with multiplicity three.

Theorem: Every irreducible cubic in the plane has a singular point or a flex. $H = det([F_{xx}, F_{yx}, F_{zx}]^T, ...)$. Flex or singular if $H = 0$.

Projective points as one dimensional subspaces. Projective lines are 1 dimensional. $n_{p \text{ on } l} n_l = n_{l \text{ on } p} n_p$.

Fundamental Theorem of Projective Geometry: Given three distinct collinear points on each of two distinct lines there is a projective transform that maps the two sets of points in the specified order.

Proof: Define $X = [1, 0, 0], Y = [0, 1, 0], Z = [0, 0, 1], U = [1, 1, 1]$.

Lemma: If $L = (P, Q, R, S)$ is a list of points of RP^2, with no three collinear, then there is a unique element of $P(2)$ mapping (X, Y, Z, U) to L.

Proof of lemma: Let P, Q, R, S be the p-points $[p]$, $[q]$, $[r]$, $[s]$ respectively. No three of P, Q, R, S are collinear, no three of p, q, r, s are linearly dependent. Suppose that t is defined by the matrix A. Then $t(U) = S$ if and only if $[Au] = [s]$, i.e. $Au = \lambda s, \lambda \neq 0$ If we replace A by $\frac{1}{\lambda}A$, we get the same t, so we may assume that $Au = s$ Now, Ax, Ay, Az are just the columns of A (in order), so t maps X, Y, Z to P, Q, R if and only if the columns of A are of the form $\alpha p, \beta q, \gamma r$, with $\alpha, \beta, \gamma \neq 0$. Also Au is the sum of the columns of A so that t has the required images if and only if $\alpha p + \beta q + \gamma r = s$. Since p, q, r are linearly independent, this has a unique solution α, β, γ. Since s is not dependent on any two of $p, q, r, \alpha, \beta, \gamma$ are non-zero. Thus the matrix A with columns $\alpha p, \beta q, \gamma r$ is invertible, so defines an element of $P(2)$. From the above argument, A is unique up to scaling, so t is unique.

By the lemma, there exist elements $r, s \in P(2)$ such that r maps (X, Y, Z, U) to L and s maps (X, Y, Z, U) to L'. Then $t = sr^{-1}$ maps L to L'. Suppose that u also maps L to L'. Then ur maps (X, Y, Z, U) to L'. By the uniqueness clause of the Theorem, only s maps (X, Y, Z, U) to L'. Thus $ur = s$, so $u = sr^{-1} = t$, i.e. t is unique.

Definition: The *cross ratio* of four points is $r = \frac{(x_1y_3 - x_3y_1)(x_2y_4 - x_4y_2)}{(x_1y_4 - x_4y_1)(x_2y_3 - x_3y_2)}$.

Theorem: Let ABC be a triangle. The medians are concurrent and divide themselves in the ratio $1:2$.

Proof: Let ABC be a triangle and let F be the median from A to BC and E be the median from C to AB; let the medians meet at G. The line EF is parallel to AC $EBF \sim ABC$ and $FEG \sim CGA$ so $EG : CG = FG : GA = 1 : 2$.

Facts: In triangle ABC, $AB + BC > AC$; if $A > B$ then $BC > AC$. A quadrilateral is cyclic if $ABCD$ lie on a circle. $ABCD$ is concyclic iff $ABC = ADB$.

Cross ratio from central projection: Let O be the center of a projection onto a line with projecting lines OA, OB, OC and OD with $ABCD$ on the line. $r = \frac{(CA)(DB)}{(CB)(DA)}$ is invariant (i.e., if A', B', C', D' are colinear and A', B', C', D' lie on OA, OB, OC, OD, respectively then $r = \frac{(C'A')(D'B')}{(C'B')(D'A')}$).

Proof: $Area(OAC) = \frac{1}{2}hCA = \frac{1}{2}(OA)(OC)sin(COA)$, $Area(OBC) = \frac{1}{2}hCB = \frac{1}{2}(OB)(OC)sin(COB)$, $Area(ODA) = \frac{1}{2}hAD = \frac{1}{2}(OA)(OD)sin(AOD)$, $Area(ODB) = \frac{1}{2}hDB = \frac{1}{2}(OB)(OD)sin(BOD)$. Dividing, we get $\frac{(CA)(DB)}{(CB)(DA)} = \frac{sin(COA)sin(BOD)}{sin(BOC)sin(AOD)}$.

Desargues: If ABC and $A'B'C'$ are perspective from a point X, then $AB \cap A'B' = P$, $AC \cap A'C' = Q$, $BC \cap B'C' = R$ are collinear.

Proof: Let ABC and abc are the two triangles with Aa, Bb, Cc concurrent. A, B, a, b are coplanar so AB and ab intersect. If both triangles are on different planes, $(AB) \cap (ab)$ is in both planes and so are $(AC) \cap (ac)$ and $(BC) \cap (bc)$ and $(BC) \cap (bc)$. These planes intersect in a line, proving the theorem.

Pappus: If ABC is on L and $A'B'C$' is on L', then $AB' \cap A'B = P$, $AC' \cap A'C = Q$, $CB' \cap C'B = R$ are collinear.

Proof: See proof below.

Ptolemy's Theorem: Let $ABCD$ be a cyclic quadrilateral (vertices lie on a circle). Then $AB \cdot CD + AD \cdot BC = AC \cdot BD$.

Proof: $CAB = BDC$ and $ADB = BCA$. Draw a line from point K to the line AC so that $ABK = DBC$. $\Delta ABK \cong \Delta DBC$ and $\Delta ABD \cong \Delta KBC$, $\frac{AK}{AB} = \frac{CD}{BD}$ and $\frac{CK}{BC} = \frac{AD}{BD}$. Thus $(AC)(BD) = (AK)(BD) + (CK)(BD) = (AB)(CD) + (BD)(DA)$.

Pascal: Suppose a hexagon is inscribed in a conic section, and opposite pairs of sides are extended until they meet in 5 points. Then if 4 of those points lie on a common line, the last point will be on that line, too.

See proof below.

Menelaus and Ceva: (1) If points X, Y, Z on BC, CA, AB (suitably extended) are collinear then $\frac{AZ}{ZB}\frac{BX}{XC}\frac{CY}{YA} = 1$. Similarly, (2) ABC with X opposite A. AX, BY, CZ are concurrent iff $\frac{AZ}{ZB}\frac{BX}{XC}\frac{CY}{YA} = 1$.

Proof: Rotate so that the line XYZ is horizontal. Drop perpendiculars from A, B, C respectively to this line with heights h_1, h_2, h_3, respectively. By similar triangles, $\frac{AY}{CY} = \frac{h_1}{h_3}$, $\frac{BZ}{AZ} = \frac{h_2}{h_1}$, and $\frac{CX}{BX} = \frac{h_3}{h_2}$. Multiply them together to get (1). For (2), note that $\frac{AZ}{BZ} = \frac{|APZ|}{|BPZ|}$, $\frac{CY}{AY} = \frac{|CPY|}{|APY|}$, and $\frac{BX}{CX} = \frac{|BPX|}{|CPX|}$. Also, $\frac{AZ}{BZ} = \frac{|AZC|}{|BZC|}$, $\frac{CY}{AY} = \frac{|CYB|}{|AYB|}$, and $\frac{BX}{CX} = \frac{|AXB|}{|AXC|}$. Thus, $\frac{BX}{CX} = \frac{|ABX|-|BPX|}{|ACX|-|CPX|} = \frac{|APB|}{|APC|}$, $\frac{CY}{AY} = \frac{|BPC|}{|BPA|}$, and $\frac{AZ}{BZ} = \frac{|APC|}{|BPC|}$. Multiplying these together we get the result.

Projective geometry with complex numbers: Points are $z \in \mathbb{C}$ and ∞. Cross ratio is $C(z_1, z_2; z_3, z_4) = \frac{(z_1-z_3)(z_2-z_4)}{(z_1-z_4)(z_2-z_3)}$. Four points lie on a line (or circle) iff their cross ratio is a real number. Moebius Transformation: $f_{a,b,c,d}(z) = \frac{az+b}{cz+d}$, $ad - bc \neq 0$. If a moebius transformation takes four points $(z_1, z_2, z_3, z_4) \mapsto (u_1, u_2, u_3, u_4)$ then $C(z_1, z_2; z_3, z_4) = C(u_1, u_2; u_3, u_4)$. Use the fact that $f_{a,b,c,d}(z) - f_{a,b,c,d}(w) = \frac{(ad-bc)(z-w)}{(cz+d)(cw+d)}$. If $C(z_1, z_2; z_3, z_4) = C(u_1, u_2; u_3, u_4)$, there is a moebius transformation that maps $(z_1, z_2, z_3, z_4) \mapsto (u_1, u_2, u_3, u_4)$.

Spherical Geometry: Let PQR be a spherical triangle with subtended angles p, q, r on a sphere of radius R. The area of PQR is $R^2(p + q + r - \pi)$.

> *Proof:* Let P', Q', R' be the antipodal points of P, Q, R respectively and C_P, C_Q, C_R be the great circles containing PP', QQ' and RR' respectively. Let Δ_C be the common area of the three great circles in the hemisphere containing P, Q, R which forms the spherical triangle. If $\Lambda(C_P, C_Q)$ is the lune formed by the intersection of the great circles, set $\Delta_1 = \Lambda(C_P, C_Q) - \Delta_C$, $\Delta_2 = \Lambda(C_P, C_R) - \Delta_C$, $\Delta_3 = \Lambda(C_R, C_Q) - \Delta_C$, and let Δ'_C, Δ'_1, Δ'_2, and Δ'_3 be the corresponding antipodal areas. $\Delta_C + \Delta_1 + \Delta_2 + \Delta_3 = \Delta'_C + \Delta'_1 + \Delta'_2 + \Delta'_3$, and $\Delta_C + \Delta_1 + \Delta_2 + \Delta_3 + \Delta'_C + \Delta'_1 + \Delta'_2 + \Delta'_3 = 4\pi R^2$ ("EQ 1"), so $\Delta_C + \Delta_1 + \Delta_2 + \Delta_3 = 2\pi R^2$. Further, $\Delta_C + \Delta_1 = 2R^2 p$, $\Delta_C + \Delta_2 = 2R^2 r$, and $\Delta_C + \Delta_3 = 2R^2 q$ so $3\Delta_C + \Delta_1 + \Delta_2 + \Delta_3 = 2R^2(p + q + r)$, subtracting EQ 1 from this and dividing by 2 gives the desired result.

Euler's Formula: $V - E + F = \chi$. For a sphere, $\chi = 2$. Let n_i: number of vertices with valence i, $2e \geq 3F$, $\sum in_i = 2E$.

Differential Geometry: Let $\mathcal{U}(\vec{x}) = \frac{\vec{x}}{|\vec{x}|}$. Curve length: $s(t) = \int_{t_0}^{t} |\gamma'(t)|dt$. $\vec{T}(t) = \mathcal{U}(\gamma'(t))$, $\vec{N}(t) = \mathcal{U}(\gamma''(t)) - \langle \gamma''(t), \vec{T}(t) \rangle \vec{T}(t)$. Alternatively, $\vec{T}(s) = \mathcal{U}(\gamma'(s))$, $\vec{N}(s) = \mathcal{U}(\vec{T}'(s))$. $\kappa(t) = \frac{\langle \vec{T}'(t), \vec{N}(t) \rangle}{\gamma'(t)}$, $\vec{B}(t) = \vec{T}(t) \times \vec{N}(t)$, $\tau(t) = \frac{\langle \vec{N}'(t), \vec{B}(t) \rangle}{|\gamma'(t)|}$. First Fundamental Form: If $E = \vec{x_u} \cdot \vec{x_u}$, $F = \vec{x_u} \cdot \vec{x_v}$ and $G = \vec{x_v} \cdot \vec{x_v}$ then $I(du, dv) = Edu^2 + 2Fdudv + Gdv^2$. If $\vec{N} = \frac{\vec{x_u} \times \vec{x_v}}{|\vec{x_u} \times \vec{x_v}|}$ then $L = -\vec{x_u} \cdot \vec{N_u}$, $M = -\frac{1}{2}(\vec{x_u} \cdot \vec{N_v} + \vec{x_v} \cdot \vec{N_u})$, $N = -\vec{x_v} \cdot \vec{N_v}$ and $II(du, dv) = Ldu^2 + 2Mdudv + Ndv^2$. $\kappa_n = \frac{II}{I}$. κ is a principal curvature iff $det \begin{pmatrix} L - \kappa E & M - \kappa F \\ M - \kappa F & N - \kappa G \end{pmatrix} = 0$. If $f(x) = 0$ defines surface, $H(f) = (\frac{\partial^2 f}{\partial x_i \partial x_j})$. *Gaussian curvature*: $det(H(f))$. If a surface is represented by $\vec{r}(u, v)$ for $(u, v) \in \mathcal{R}$ then $A(S) = \int_{\mathcal{R}} |\frac{\partial \vec{r}}{\partial u} \times \frac{\partial \vec{r}}{\partial v}| \, du \, dv$. *Torus:* $\vec{r}(\theta, \phi) = ((R + rcos(\phi))cos(\theta), (R + rcos(\phi))sin(\theta), Rsin(\phi))$. $A(S) = 4\pi^2 rR$.

Model for Hyperbolic Geometry: $\mathcal{H} = \{x + yi : y > 0\}$ is the *hyperbolic plane*. *Hyperbolic lines* are semicircles with centers on the real axis. Mobieus transformations fix $\mathcal{H}$ and map hyperbolic lines to hyperbolic lines. If $[a, b, c, d]$ is the cross ratio, the hyperbolic distance between z_1 and z_2 is $log([u, z_1, z_2, v])$ where u and v are the endpoints on the real line of the hyperbolic line joining z_1 and z_2. If a hyperbolic right trainagle consists of lines of length a, b, c, $cosh(c) = cosh(a) \cdot cosh(b)$. Any bijection mapping circles into cirlces is a Mobieus transformation on z or $\overline{z}$.

Gaussian curvature: If k_1 and k_2 are the maximum and minimum values of the curvature at a point on a surface, the Gaussian curvature is $K = k_1 k_2$; $\chi = 2 - 2g$ is the Euler characteristic, where g is the genus. k_1 and k_2 are also eigenvalues of the *Hessian*. The *genus* of a connected, orientable surface is an integer representing the maximum number of cuttings along closed simple curves without rendering the resultant manifold disconnected and it is equal to the number of handles on it.

Gauss-Bonnet: If X is a compact, hypersurface in $\mathbb{R}^{k+1}$, then $\int_X K = Vol(S^k)\frac{\chi(X)}{2}$.

Eight Point Theorem: Suppose C is a curve in $\mathbb{P}^2_K$ defined by homogeneous cubic polynomial $C(x,y,z) = 0$. Let l_1, l_2, l_3 and m_1, m_2, m_3 be lines in $\mathbb{P}^2_K$ with $l_i \neq m_j, \forall i,j$ and $P_{ij} = l_i \cap m_j$. Suppose further that C is not singular at $P_{ij}, \forall i,j \neq 3,3$. Then $P_{33} \in C$. This is proved in a series of lemmas. *Lemma 1:* Let $P_{i1} = (u_i : v_i)$ and $m_j : a_j x + b_j y + c_j z = 0$, $\overline{m_j}(u_i, v_i) = 0$ and $\overline{m_j}$ vanishes only at P_{ij}. $\overline{m_1}(u,v)\overline{m_2}(u,v)\overline{m_3}(u,v)$ is a homogeneous cubic polynomial. *Lemma 2:* If $R(u,v), S(u,v)$ are homogeneous of degree 3 and is not identically 0 and they both vanish at $(u_i : v_i)$ then $\exists \alpha \in K, \alpha \neq 0$: $R = \alpha S$. *Lemma 3:* $\overline{C} = \alpha\overline{m_1}(u,v)\overline{m_2}(u,v)\overline{m_3}(u,v)$ and $\overline{C} = \alpha\overline{l_1}(u,v)\overline{l_2}(u,v)\overline{l_3}(u,v)$. *Lemma 4:* $l_i \mid (C - \alpha m_1(u,v)m_2(u,v)m_3(u,v))$, $m_j \mid (C - \beta l_1(u,v)l_2(u,v)l_3(u,v))$ and if $D = C - \alpha m_1(u,v)m_2(u,v)m_3(u,v) - \beta l_1(u,v)l_2(u,v)l_3(u,v)$, then $l_i m_j \mid D$. *Lemma 5:* $D = l_1 m_1 l(u,v)$ and $l(P_{22}) = l(P_{23}) = l(P_{32}) = 0$, so $D = 0$. To conclude the proof of the eight point theorem, observe, since $D = 0$, $C = \alpha m_1(u,v)m_2(u,v)m_3(u,v) + \beta l_1(u,v)l_2(u,v)l_3(u,v)$ and $l_3(P_{33}) = m_3(P_{33}) = 0$ thus $C(P_{33}) = 0$.

The eight point theorem proves associativity of elliptic curve addition: Let P, Q, R be points on C and consider $l_1 = \overline{P,Q}$, $l_2 = \overline{\infty, Q+R}$, $l_3 = \overline{R, P+Q}$, $m_1 = \overline{Q,R}$, $m_2 = \overline{\infty, P+Q}$, $m_3 = \overline{P, R+Q}$. $l_1 \cap m_1 = Q$, $l_1 \cap m_2 = -(P+Q)$, $l_1 \cap m_3 = P$, $l_2 \cap m_1 = -(Q+R)$, $l_2 \cap m_2 = \infty$, $l_2 \cap m_3 = Q+R$, $l_3 \cap m_1 = R$, $l_3 \cap m_2 = (P+Q)$, $l_3 \cap m_3 = X$. X is $-((P+Q)+R)$ (from the definition of l_3) and $-(P+(Q+R))$ (from the definition of m_3) by the definition of addition. Now apply the eight point theorem to get the result.

The eight point theorem also proves **Pascal's Theorem:** Let $ABCDEF$ be a hexagon inscribed in a conic section whose equation is $Q(x,y,z) = 0$. If $X = \overline{AB} \cap \overline{DE}$, $Y = \overline{BC} \cap \overline{EF}$, $Z = \overline{CD} \cap \overline{FA}$, then X, Y, Z are collinear.

> *Proof:* Put $l_1 = \overline{EF}$, $l_2 = \overline{AB}$, $l_3 = \overline{CD}$, $m_1 = \overline{BC}$, $m_2 = \overline{DE}$, $m_3 = \overline{FA}$, $C(x,y,z) = Q(x,y,z)l(x,y,z)$ and apply the theorem.

This also proves **Pappus's Theorem:** Let l, m be two distinct lines A, B, C on l and A', B', C' on m none of which are on $l \cap m$. If $X = \overline{AB'} \cap \overline{A'B}$, $Y = \overline{BC'} \cap \overline{B'C}$, $Z = \overline{CA'} \cap \overline{C'A}$, then X, Y, Z are collinear. *Proof:* Use Pascal with hexagon $AB'CA'BC'$.

Definition: Let $\Phi : Q \to P$ be a *homotopy* of φ_0 into φ_1 as closed curves and let $y \notin \Phi(Q)$. Then the *winding number* $W(\varphi_r, y)$ is constant for $0 \leq r \leq 1$. Let φ be a closed curve $\varphi : [a,b] \to P$ and suppose y_0, y_1 can be joined by a curve which does not intersect φ, then $W(\varphi, y_0) = W(\varphi, y_1)$. Let $f : D \to P$ be a mapping of the disk onto the plane and let $C = \partial D$ and let $y \notin f(C)$; if the winding number of $f|C$ about y is not zero, then $y \in f(D)$ such that $f(x) = y$. Let $f : D \to P$ be a mapping of a disk onto a plane, P and $C = \partial D$ that fixes all of C then $D \subseteq f(D)$. No mapping of a disk onto its boundary fixes each point of the boundary. If f is a mapping of a disk onto itself, it has a fixed point.

Theorem: A finite group of transformations over $\mathbb{R}^3$ has fixed points. $|G| = v_p n_p$, $2(|G|-1) = \sum_p (v_p - 1)$.

1.3.2 Real Analysis and Manifolds

Definition: A metric space, R, is a vector space with a distance $d : R \times R \to \mathbb{R}^{\geq 0}$, such that $d(x,x) = 0$ iff $x = 0$ and $\forall x, y, z \in R$, $d(x,z) \leq d(x,y) + d(y,z)$. $B_r(c) = \{x : d(x,c) \leq r\}$

Definition: A set $S \subseteq R$ in a metric space R is open if $\forall x \in R, \exists \epsilon > 0 : B_\epsilon \subseteq S$. T is a closed set if $R \setminus S$ is open. A subset $S \subseteq R$ if every open cover of S contains a finite subcover of S.

Theorem: (a) S is compact iff S is closed and bounded; (b) $[a,b]$ is compact; (c) if f is continuous, $f([a,b])$ is compact; (d) if S is closed and $lim_{n\to\infty}x_n = a, x_n \in S$ then $a \in S$.

Proof: (a, $\to$) Suppose S is a compact set and suppose $\overline{S}$ is not open. There is a point $X \in \overline{S}$ which contains no open ball, $B_r(X)$. Let $R_x = \{y \in S : d(x,y) < \frac{d(x,X)}{2}$ then $\{R_x, x \in S\}$ is an open cover of S with no finite subcover, so no such X exists and $\overline{S}$ is open so S is closed. If S is not bounded then $R_{x,n} = \{y \in S : d(x,y) < n\}$, $\{R_{x,n}, x \in Sn \in \mathbb{Z}\}$ is an open cover with no finite subcover so S must be bounded. (a, $\leftarrow$) Suppose S is a closed, bounded set which is not compact and let U be an open cover of S. Since S is bounded there are a finite number of closed balls $\overline{B_{\frac{1}{2}}(a_i)}, a = 1, 2, \ldots, k$. At least one of $S_1 = S \cap \overline{B_{\frac{1}{2}}(a_i)}$, say $\overline{B_{\frac{1}{2}}(a_j)}$, which does not have a finite subcover. Repeating this argument, with $S_2 = \overline{B_{\frac{1}{4}}(a_j)}, \ldots, S_k\overline{B_{\frac{1}{2^k}}(a_j)}, \ldots,$. $S_1 \supseteq S_2 \supseteq \ldots$. The common interesection contains a point $p \in S$. Since U contains an open subset T, $p \in T$, the chain of subsets terminates after finitely many terms contradicting the assumption that no finite subcover exists. (b) $[a,b]$ is closed and bounded and the result follows from (a). (c) If U is a cover of $f([a,b])$; then $W = \{f^{-1}(X), X \in U\}$ is a cover of $[a,b]$, so there is a finite subcover $W_1 \subseteq W$ but then $\{f(Y), Y \in W_1\}$ is a finite cover of $f([a,b])$. (d) If $lim_{n\to\infty}x_n = a, x_n \in S$ then any open set containing a has a non trivial intersection with S and so $\overline{S}$ is not open if $a \in \overline{S}$.

Theorem: If f is continuous on $[a,b]$ and $f(a) = f(b)$ then f attains a maximum (minimum) at some point, $c : a < c < b$ and if f is differentiable, $f'(c) = 0$. $\exists \xi, a < \xi < b$ such that $f'(\xi) = \frac{f(b)-f(a)}{b-a}$.

Proof: Set $g(x) = f(x) - [(\frac{f(b)-f(a)}{b-a})(x-a) + f(a)]$. $g(a) = g(b) = 0$ and there is a $a < \xi < b$ on which g attains a maximum or minimum. $g'(\xi) = 0 = f'(\xi) - \frac{f(b)-f(a)}{b-a}$.

Definition: f is *convex upwards* (resp *convex downwards*) on $[a,b]$ if $f(at + (1-t)b) \leq tf(a) + (1-t)f(b)$ for $0 \leq t \leq 1$ (resp. $f(at + (1-t)b) \geq tf(a) + (1-t)f(b)$ for $0 \leq t \leq 1$).

Theorem: If $f''(x) > 0$ (resp $f''(x) < 0$, $a \leq x \leq b$) then f is convex upwards (resp convex downwards).

Proof (convex backwards): Put $g(t) = f(ta + (1-t)b) - tf(a) + (x-1)f(b)$. $g(0) = g(1) = 0$. $g''(t) = (a-b)^2 f''(ta + (1-t)b)$. If g has a local minumum at t_0, $g(t_0) = 0$ and $g''(t_0) > 0$. This is a contradiction so the minumum of $g, 0 \leq t \leq 1$ occurs at the endpoints and the result holds.

Definition A space is connected iff it cannot be written as a disjoint union of relatively open sets.

Theorem: If f is continuous and E is a connected space, so is $f(E)$.

Proof: Suppose $f(E) = X \cup Y$, then $f^{-1}(X) \cup f^{-1}(Y) = f(E)$ and they are disjoint, relatively open sets.

Theorem: If φ is strictly increasing and $\varphi : [A,B] \to [a,b]$ and α is also increasing on $[a,b]$, set $\beta(y) = \alpha(\varphi(y))$ and $g(y) = f(\varphi(y))$ then $\int_A^B g\, d\beta = \int_a^b f\, d\alpha$.

Fundamental Theorem of Calculus: Suppose f is integrable on $[a,b]$ and define $F(x) = \int_a^x f(t)\, dt$ then for $a \leq c \leq b$, we have $F'(c) = f(c)$ and $\int_a^b f(t)\, dt = F(b) - F(a)$.

Proof: $F(x+h) - F(x) = \int_x^{x+h} f(x)dx$, $\exists c : x \leq c \leq x+h : \int_x^{x+h} f(x)dx = hf(c)$. So $lim_{h\to 0}\frac{F(x+h)-F(x)}{h} = f'(x)$.

Definition: A sequence $\{f_n\}$ converges *uniformly* on E to f if $\forall \epsilon > 0, \exists N : n > N, |f(x) - f_n(x)| < \epsilon$. A family $\mathcal{F}$ is *equicontinuous* on E if $\forall \epsilon > 0, \exists \delta > 0 : |f(x) - f(y)| < \epsilon$ if $|x - y| < \delta, \forall f \in \mathcal{F}$.

Theorem: If a sequence of continuous functions $\{f_n\}$ converges uniformly to f on E then f is continuous on E.

Proof: Choose $N : \forall n \geq N, |f_n(x) - f(x)| < \frac{\epsilon}{3}$ and choose $\delta > 0 : |f_n(x+h) - f_n(x)| < \frac{\epsilon}{3}$. $|f(x+h) - f(x)| \leq |f_n(x+h) - f(x+h)| + |f_n(x) - f(x)| + |f_n(x+h) - f_n(x)| < \epsilon$ for the chosen δ.

Theorem: If K is compact and a sequence of continuous functions $\{f_n\}$ converges pointwise to f on K and if $f_n(x) \geq f_{n+1}(x)$ then $\{f_n\}$ converges *uniformly* on K.

Theorem: If K is compact and $\{f_n\}$ converges uniformly then $\{f_n\}$ is equicontinuous.

Theorem: If K is compact and $\{f_n\}$ converges pointwise on K then $\{f_n\}$ is uniformly bounded and $\{f_n\}$ contains a uniformly convergent subsequence.

Stone Weierstrauss Theorem: If f is continuous on K, compact, $\exists P_n \in \mathbb{R}[x]$ such that $\lim_{n\to\infty} P_n(x) = f(x)$.

Lemma: The Stone Weierstauss Theorem holds if $f, g \in \overline{\mathbb{R}[x]} \to max(f,g), min(f,g) \in \overline{\mathbb{R}[x]}$.

Proof of Lemma: $\forall \alpha, \beta$, if $x_1 \neq x_2$, $\exists h \in \overline{\mathbb{R}[x]}$ such that $h(x_1) = \alpha$ and $h(x_2) = \beta$. To show this, pick $\phi \in \mathbb{R}[x] : \phi(x_1) \neq \phi(x_2)$ then put $h(x) = \alpha + \beta \frac{\phi(x) - \phi(x_1)}{\phi(x_2) - \phi(x_1)}$. Next we show that if f is continuous on S then, $\forall \epsilon > 0, \forall z \in \overline{\mathbb{R}[x]}, \exists g \in \overline{\mathbb{R}[x]} : f(z) - \epsilon < g(z) < f(z) + \epsilon$. Let $h_{x,y}(z)$ be a function with $h_{x,y}(x) = f(x)$ and $h_{x,y}(y) = f(y)$. Such a function exists by the first part of this proof. Let U_x be a open neighborhood of x in which $h_{x,y}(z) < f(z) + \epsilon$ which exists by continuity. There is a finite subcover of U_x, $U_{x_1}, \ldots, U_{x_n}$. Put $g = min(h_{x_1,y}, \ldots, h_{x_n,y})$. Let V_y be a open neighborhood of y in which $f(z) - \epsilon < h_{x,y}(z)$, again we can find a finite subcover and putting $g = max(h_{x,y_1}(z), \ldots, h_{x,y_m}(z))$, we get $f(z) < g(z) - \epsilon$. $f(z) - \epsilon < g(z) < f(z) + \epsilon$, proving the lemma. Note that $\sum_{i=0}^{n} \binom{n}{i} f(\frac{i}{n}) x^i (1-x)^{n-i}$ is a good approximation of f.

Proof of Stone Weierstrauss: Since $max(f,g) = |f|+|g|+|f-g|$ and $mix(f,g) = |f|+|g|-|f-g|$, it suffices to show $h(x) = |x| \in \overline{\mathbb{R}[x]}$. Then $\forall \epsilon > 0, \exists P : |P(t) - |t|| < \epsilon$ and so $|P(f(x)) - |f(x)|| < \epsilon$. Thus, $P(f(x)) \in \overline{\mathbb{R}[x]}$.

Theorem: Let $\mathcal{A}$ be an algebra of real continuous functions on a compact set K. If $\mathcal{A}$ separates points and vanishes at no point then the uniform closure of $\mathcal{A}$ consists of all real continuous functions.

Taylor's Theorem: $f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k + \frac{f^{(n+1)}(c)}{(n+1)!}(x-a)^{n+1}$ for some $c : a < c < x$.

Proof: Set $F(t) = \sum_{k=0}^{n} \frac{f^{(k)}(t)}{k!}(x-t)^k$ and let $E_n(x) = f(x) - \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k$. Note $F(x) - F(a) = E_n(x)$ and $F'(t) = \frac{f^{(n+1)}(t)}{n!}(x-t)^n$. Put $G(t) = (x-t)^{n+1}$ and $H(t) =$

$G(t)[F(x)-F(a)]-F(t)[G[x]-G(a)]$. $H(a)=H(x)$ so $\exists c: a<c<x$ with $H'(c)=0$. So $E_n(x)=F(x)-F(a)=\frac{F'(c)}{G'(c)}[G(x)-G(a)]$. Substituting gives the desired result.

Another proof: $b=a+h$, $f(b)=f(a)+\frac{(b-a)}{1!}f^{(1)}(a)+\ldots+\frac{(b-a)^n}{n!}f^{(n)}(a)+R_n(a)$. Regard b as constant and differentiate with respect to a. By repeated application of the product rule, we get $0=R_n'(a)+\frac{(b-a)^n}{n!}f^{(n+1)}(a)$. Integrating (and switching limits), we get $R_n(a)=\int_a^b\frac{(b-t)^n}{n!}f^{(n+1)}(t)dt$. Applying the generalized mean value theorem ($p(x)>0\rightarrow\int_a^b f(x)p(x)dx=f(\xi)\int_a^b p(x)dx, a\leq\xi\leq b$), we get $R_n(a)=\frac{1}{n!}f^{(n+1)}(\xi)\int_b^a(b-t)^n dt=\frac{1}{(n+1)!}f^{(n+1)}(\xi)(b-a)^{n+1}$.

A third proof: We proceed by induction. We want to show $f(a+h)=f(a)+\sum_{i=1}^n\frac{h^i}{i!}f^{(i)}(a)+R_n$, where $R_n=\int_a^{a+h}f^{(n+1)}(t)\frac{(a+h-t)^n}{n!}dt$. For $n=0$, $f(a+h)-f(a)=\int_a^{a+h}f'(t)dt$ is just the FTOC. For step $n+1$, we have from step n that $f(a+h)-f(a)-\sum_{i=1}^n\frac{h^i}{i!}f^{(i)}(a)=\int_a^{a+h}f^{(n+1)}(t)\frac{(a+h-t)^n}{n!}dt$. Integrate by parts with $u=f^{(n+1)}(t)$ and $v=-\frac{(a+h-t)^{n+1}}{(n+1)!}$. This gives $f(a+h)-f(a)-\sum_{i=0}^{n+1}f^{(i)}(a)\frac{h^i}{i!}=\int_a^{a+h}\frac{(a+h-t)^{n+1}}{(n+1)!}f^{(n+2)}(t)dt$ which is the result for $n+1$.

Definition: X separates if $\exists A,B, A\neq X,\emptyset, \exists B\neq X,\emptyset$ both open with $A\cup B=X$ and $A\cap B=\emptyset$. X is connected iff there is no separation. Suppose $f:X\rightarrow Y$ is *continuous.* If X is compact so is $f(X)$. If X is connected, so is $f(X)$. If X compact, *connected* set in $\mathbb{R}$ then $X=[a,b]$.

Some identities: $\int_{-\pi}^{\pi}cos(mx)cos(nx)dx=\int_{-\pi}^{\pi}sin(mx)sin(nx)dx=\delta_{mn}\pi$. *Bernoulli:* $\phi_n'(x)=\phi_{n-1}(x), \phi_0(x)=1, \int_0^1\phi_n(x)dx=1$. $\Gamma(x)=\int_0^\infty u^{x-1}e^{-u}du$.

Optimization: f has a global minimum if it is *convex.* f is convex iff its *Hessian* is positive semi-definite. An optimization problem is convex if the objective function and the constraints are convex. Convex optimization problems have global minimums.

Fixed Point Theorem: Let E be a complete metric space and $f:E\rightarrow E$. Suppose $\exists k<1:\forall p,q\in E, ||f(p)-f(q)||\leq k||p-q||$. Then there is a unique $P\in E: f(P)=P$.

Proof: Let $p_{n+1}=f(p_n)$. $||f(p_{n+1})-f(p_n)||\leq k||p_n-p_{n-1}||\leq k^n||p_1-p_0||$. This is a Cauchy sequence and converges. Set $p=lim_{n\rightarrow\infty}p_n$, $f(p)=p$. Uniqueness: if q is another such point: $||f(p)-f(q)||=||p-q||\leq k||p-q||$ so $||p-q||=0$.

Simple Implicit Function Theorem: Let f be a real valued continuous function on an open set $E\subset\mathbb{R}^2, (a,b)\in E$ with continuous partial $\frac{\partial f}{\partial y}(a,b)\neq 0$. There are open sets U,V with $a\in U, b\in V$ and a continuous function $\varphi:U\rightarrow V$ such that $f(x,\varphi(x))=0, x\in U$.

Proof: Define $F(x,y)=y-f(x,y)(\frac{\partial f}{\partial y})^{-1}$. $F(a,b)=b$, $\frac{\partial F}{\partial y}(a,b)=0$ and $F(x,y)=y$ iff $f(x,y)=0$. Pick r small enough so that in the ball $B_r(a,b): |\frac{\partial F}{\partial y}|<\frac{1}{2}$. Choose $k: 0<k<r$ then choose $h: 0<h<\sqrt{r^2-k^2}$ such that $|F(x,b)-b|<\frac{k}{2}$ when $|x-a|<h$. Put $U=(a-h,a+h), V=(b-k,b+k)$. Fix $x\in U$ and $|y-b|\leq k$ and suppose $||(x,y)-(a,b)||^2<h^2+k^2<r^2$ and $||(x,y')-(a,b)||^2<h^2+k^2<r^2$. $\exists y'': |F(x,y)-F(x,y')|\leq\frac{\partial F}{\partial y}(x,y'')|y-y'|\leq\frac{1}{2}|y-y'|$ and $|F(x,y)-b|\leq|F(x,y)-F(x,b)|+|F(x,b)-b|<k$. Apply Fixed Point Theorem to get $\overline{y}=f(x,\overline{y})$. This is unique. Define $\varphi(x)=\overline{y}$. A simple argument shows φ is continuous.

Simple Inverse Function: Let g be a real valued function on an open set $E\subset\mathbb{R}$ and suppose g' exists and is continuous in E and $g'(b)\neq 0$. There are open sets $U,V\subset\mathbb{R}$ with $b\in V: g_{|V}$ is 1-1 and $g^{-1}:U\rightarrow V$

is differentiable. *Proof:* Put $f(x,y) = x - g(y)$ and apply the implicit function theorem.

Existence of solution to ordinary differential equation: Let f be a continuous real valued function in an open set $E \subset \mathbb{R}^2$ containing (a,b) and suppose $\exists M : |f(x,y) - f(x,z)| < M|y-z|, (x,y), (x,z) \in E$ then $\exists h > 0$ and $\varphi : (a-h, a+h) \to (b-M, b+M) : \varphi'(x) = f(x, \varphi(x))$ on $(a-h, a+h)$ and $\varphi(a) = b$.

> Proof: This is equivalent to $\varphi(x) = \int_a^x f(t, \varphi(t))dt + b$. Suppose ψ is a function and define $F : \psi \mapsto \int_a^x f(t, \psi(t))dt + b$. F maps the complete metric space of functions on a closed interval of E itself. A fixed point in this metric space would satisfy the theorem; we show such a fixed point exists. Choose $N > |f(a,b)|, \exists r : ||(x,y) - (a,b)|| < r \to |f(x,y)| < N$. Choose $h > 0 : h < \frac{r}{2N}, h < \frac{1}{2}, hM < 1$ and consider the complete metric space of continuous functions on $[a-h, a+h]$ denoted by $\mathcal{C}([a-h, a+h])$; define $R = \{(x,y) \in E : |a-x| \leq h, |y-b| \leq Nh\}$ and $B = \{\psi : [a-h, a+h] \to [b-Nh, b+Nh]\}$, finally, Let $B_{Nh}(b)$ be the ball in $\mathcal{C}([a-h, a+h])$ of functions within Nh of the constant function b. For $\psi, \omega \in B_{Nh}(b)$ note that $|\psi(x) - b| < Nh$ and $f(t, \psi(t)) < N$ so $|F\psi(x) - b| < Nh$. For $\psi, \omega \in B_{Nh}(b) : |F\psi(x) - F\omega(x)| \leq hM||\psi - \omega||$. This satisfies the conditions of the fixed point theorem and the fixed point satisfies the conclusion of the theorem.

Implicit Function Theorem: Let $a \in E^m \subset \mathbb{R}^m$ and $b \in E^n \subset \mathbb{R}^n$ with $(a,b) \subset E^{m+n}$, and open set. Suppose $f_1(a,b) = \ldots = f_n(a,b) = 0$ and $\frac{\partial f_i}{\partial y_j}$ exist and are continuous in E^{m+n} and $det(\frac{\partial f_i}{\partial y_j}(a,b)) \neq 0$ then $\exists U^{open} \subset E^m, a \in U, V^{open} \subset E^n, b \in V, \varphi : U \to V$ such that $f_i(x, \varphi(x)) = 0$ for $i = 1, 2, \ldots, n$.

> *Proof:* Define $x = \vec{x} = (x_1, \ldots, x_m)$, $y = \vec{y} = (y_1, \ldots, y_n)$ and $F = \vec{F} = (F_1(\vec{x}, \vec{y}), \ldots, F_n(\vec{x}, \vec{y}))$. Define $F_i(x,y) = y_i - \sum_j c_{ij} f_j(x,y)$ with each partial continuous. (1) The F_i are continuously differentiable; (2) $F_i(a,b) = b$; (3) $\frac{\partial F_i}{\partial y_j}(a,b) = 0$; (4) $f_i(x,y) = 0$ iff $F_i(x,y) = y_i$. For 3 to hold (c_{ij}) must be the inverse of the Jacobian. For 4 to hold, the determinant of the Jacobian must be $\neq 0$. Choose $r > 0$ such that for $(x,y) \in B_r(a,b) \subset E^{m+n}$, $|\frac{\partial F_i}{\partial y_j}| < \frac{1}{2n^2}$ and $det(\frac{\partial F_i}{\partial y_j}) \neq 0$. Choose $k : 0 < k < r$ and choose h so that $0 < h < \sqrt{r^2 - k^2}$ and $||F(x,b) - b|| < \frac{k}{2}$ if $||x - a|| < h$. Fix $x \in U$ with $||(x,y) - (a,b)|| < r$. If $y' \in E^n, ||y' - b|| \leq k, \exists y'' : F(x,y) - F(x,y') = (y - y') \cdot (\frac{\partial F_1(x,y'')}{\partial y_1}, \ldots, \frac{\partial F_n(x,y'')}{\partial y_n}) \leq \frac{1}{2n^2}(|y_1 - y_1'| + \ldots + |y_n - y_n'|) \leq \frac{1}{2n}||y - y'||$. So $||F(x,y) - F(x,y')|| < k$ and the fixed point theorem applies.

Extended Inverse Function Theorem: $f_i(x,y) = x_i - g_i(y), a = g(b)$. Same deal.

Inverse Function Theorem: Suppose $f : \mathbb{R}^n \to \mathbb{R}^n$ is continuously differentiable and $|det(f'(a)| \neq 0$. $\exists V^{open}, W^{open}, f^{-1}, a \in V, f(a) \in W$ with $f^{-1} : W \to V$ and $f^{-1}(f(x) = x$. Further $f'^{-1}(y) = \frac{1}{f'(f^{-1}(y))}$. Notes: Let $\lambda = D(f(a))$. May assume $\lambda = I$. Can show $|x_1 - x_2| \leq |f(x_1) - f(x_2)|$.

Implicit Function Theorem: If $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^m$ is continuously differentiable in an open set containing $(a,b), f(a,b) = 0$ with $M = (D_{n+j}(f^i(a)))$ with $1 \leq i, j \leq m$. If $det(M) \neq 0, \exists A^{open} \subseteq \mathbb{R}^n$ and $B^{open} \subseteq \mathbb{R}^m, a \in A, b \in B : \forall x \in A$ there is a unique $g(x) \in B, f(x, g(x)) = 0$. Further, g is differentiable. Notes: Look at $F(x,y) = (x, f(x,y))$ and apply Inverse Function Theorem.

Partitions of unity: $A^{open} \subseteq \mathbb{R}^n$ and $\mathcal{O}$ and open cover of A. $\exists \Phi \in \mathbb{C}^\infty$ such that $\forall \varphi \in \Phi$: (1) $0 \leq \varphi(x) \leq 1$ and $\forall x \in A$, (2) $\forall x, \varphi(x) = 0$ for all but finitely many $\varphi \in \Phi$, (3) $\sum_{\varphi \in \Phi} \varphi(x) = 1$. (4) $\forall \varphi \in \Phi, \exists U^{open} \in \mathcal{O} : \phi(x) = 0$ for $x \notin \overline{U}$ where $\overline{U}$ is some closed subset of U.

Direct proof of inverse function theorem: Suppose f is a $\mathcal{C}'$ mapping $f : E \to \mathbb{R}^n$, $a \in E^{open} \subseteq \mathbb{R}^n$

with $f'(a)$ invertible and $f(a) = b$, then (a) $\exists U^{open}, V^{open} \subseteq \mathbb{R}^n : a \in U, b \in V$ such that f is 1-1 on U; $f(U) = V$. (b) If $g = f^{-1}$ then $g \in \mathcal{C}'(V)$.
Proof of a: Put $f'(a) = A$ and choose $\lambda : 2\lambda||A^{-1}|| = 1$, set $U = B_\lambda(a) \subseteq E$: $||f'(x) - A|| < \lambda, \forall x \in U$. Set $\varphi_y(x) = x + A^{-1}(y - f(x)), \forall y \in \mathbb{R}^n$. $||\varphi_y'(x)|| = ||A^{-1}(A - f'(x))|| < \frac{1}{2}$. $||\varphi_y(x_1) - \varphi_y(x_2)|| < \frac{1}{2}, \forall x_1, x_2 \in U$ [Equation 1] by the mean value theorem. φ_y is a contraction map so it has a unique fixed point $x : y = f(x)$. Put $V = f(U)$ and suppose $y_0 \in V$, there is a $x_0 \in U : y_0 = f(x_0)$. Pick $r > 0 : \overline{B_r(x_0)} \subseteq U$. Fix $y : |y - y_0| < \lambda r$. For $x \in \overline{B_r(x_0)}$, $|\varphi(x_0) - x_0| \leq |\varphi(x) - \varphi(x_0)| + |\varphi(x_0) - x_0| < \frac{1}{2}|x - x_0| + \frac{r}{2} \leq r$ so $\varphi(x) \in \overline{B_r(x_0)}$ and again φ_y is a contraction map. Its fixed point x satisfies $f(x) = y, y \in \overline{B_r(x_0)} \subseteq f(U) = V$, so V is open.
Proof of b: Pick $y \in V$, $y + k \in V, \exists x, x + h \in U : y = f(x), y + k = f(x + h)$. Now $\varphi(x + h) - \varphi(x) = h + A^{-1}(f(x + h) - f(x)) = h - A^{-1}(f(x + h) - f(x)) = h - A^{-1}k \leq \frac{1}{2}h$ by equation 1, so $||A^{-1}k|| \geq \frac{||h||}{2}$ and $||h|| \leq 2||A^{-1}k|| = \lambda^{-1}||k||$. $f'(x)$ has an inverse T and $g(y + k) - g(y) - Tk = h - Tk = -T[f(x + h) - f(x) - f'(x)h]$ and $\frac{||g(y+k)-g(y)-Tk||}{||k||} = \frac{||T||}{\lambda} \frac{||f(x+h)-f(x)-f'(x)h||}{||h||}$. Now $h \to 0$ as $k \to 0$. Since the right hand side goes to 0, the left hand side goes to 0 and we get $g'(y) = T$.

Fubini's Theorem: $\int\int_{I^2} f(x, y)dydx = \int_0^1 (\int_0^1 f(x, y)dy)dx$. In a simply connected region of the plane, S for $a \leq x \leq b$ bounded by $b_1(x) \leq y \leq b_2(x)$, $\int\int_S f(x, y)dydx = \int_a^b (\int_{b_1(x)}^{b_2(x)} f(x, y)dy)dx$.

> *Proof:* Partition the region in steps of Δx and Δy. Summing over rectangles in the y direction moving and then moving in the positive x direction gives the result.

Change of variables: Let $A \subseteq \mathbb{R}^n$ be an open set, $g : A \to R$ continuously differentiable and $det(g'(x)) \neq 0, \forall x \in A$. If $f : g(A) \to R$ is integrable then $\int_{g(A)} f = \int_A f \circ g |\det(g')|$.

> *Proof:* If A is an $n \times n$ matrix. $det(A)$ is the volume of the image of the unit n-cube under A. Todo.

Let $\mathcal{T}^k(V) = \{T : V \to \mathbb{R}\}, V \subseteq \mathbb{R}^n$ where $\forall i$: $T(v_1, ..., v_{i-1}, u+w, v_{i+1}, ..., v_k) = T(v_1, ..., v_{i-1}, u, v_{i+1}, ..., v_k) + T(v_1, ..., v_{i-1}, w, v_{i+1}, ..., v_k)$ and $T(v_1, ..., v_{i-1}, au, v_{i+1}, ..., v_k) = aT(v_1, ..., v_{i-1}, u, v_{i+1}, ..., v_k)$. $\mathcal{T}^n(V)$ are called the $n-$tensors V. If $f : V \to W$ with $V, W \subseteq \mathbb{R}^n$ then $f^* : \mathcal{T}^n(W) \to \mathcal{T}^n(V)$ by $f^*(T(v_1, ..., v_n)) = T(f(v_1), ..., f(v_n))$. If $T \in \mathcal{T}^k, S \in \mathcal{T}^s$ define $T \otimes S = T(x_1)S(x_2)$. $\mathcal{T}^1(V)$ is just the dual space V^*. If $e_1, ..., e_n$ is a basis for V and $\varphi_j \in V^*$ such that $\varphi_j(e_i) = \delta_{ij}$ then the set of all $k - fold$ tensor products $\varphi_{i_1} \otimes \varphi_{i_2} \otimes ... \otimes \varphi_{i_k}$ is a basis $\mathcal{T}^k(V)$ which thus has dimension n^k.

Definition: An *alternating form* is a multilinear function, $\Lambda^k(V) = \{T \in \mathcal{T}^k(V)\}$ such that $T(...v...w...) = -T(...w...v...)$. $\forall T \in \mathcal{T}^n(V), Alt(T) = \frac{1}{k!} \sum_\sigma sgn(\sigma)T(v_{\sigma(1)}, ..., v_{\sigma(n)}) \in \Lambda^k(V)$. If $\omega \in \Lambda^k(V)$, $Alt(\omega) = \omega$. If $\omega, \eta \in \Lambda^k, \Lambda^l$, $\omega \wedge \eta = \frac{(l+k)!}{k!l!} Alt(\omega \otimes \eta)$. $\wedge$ is multilinear and $\omega \wedge \eta = (-1)^{kl}\eta \wedge \omega$; $f^*(\omega \wedge \eta) = f^*(\omega) \wedge f^*(\eta)$. $(\omega \wedge \eta) \wedge \theta = \omega \wedge (\eta \wedge \theta) = \frac{(k+l+m)}{k!l!m!} Alt(\omega \otimes \eta \otimes \theta)$. If $\omega = \sum w_{i_1,...i_k} dx^{i_1} \wedge ... \wedge x^{i_k}$ then $d\omega = \sum dw_{i_1...i_k} \wedge dx^{i_1} \wedge ... \wedge x^{i_k}$. $dim(\phi_{i_1} \wedge ... \wedge \phi_{i_k}) = \binom{n}{k}$. orientation: $[e_1, ..., e_n]$. *Volume elements:* $w_i = \sum_j a_{ij} v_j$ then $\omega(w_1, ..., w_n) = det(a_{ij})\omega(v_1, ..., v_n)$ for $\omega \in \Lambda^k$.

Forms: Let $p, v \in \mathbb{R}^n$, define the tangent space of $\mathbb{R}^n$ at p, ${\mathbb{R}^n}_p$, as the (p, v) with $(p, v) + (p, w) = (p, v + w)$ and $(p, av) = a(p, v)$.

Vector field: $F(p) = F^1(p)(e_1)p + ... + F^n(p)(e_n)p$ with the usual rules $(F + G)(p) = F(p) + G(p)$ $(f \cdot g)(p) = f(p) \cdot g(p)$. $\nabla = \sum D_i \cdot e_i$.

Differentials: $\omega(p) \in \Lambda^k({\mathbb{R}^n}_p)$: If $\varphi_i(p)$ is the dual basis for $(e_1)_p, (e_2)_p, ..., (e_n)_p$ then $\omega(p) = \sum \omega_{i_1,...i_k} \varphi^{i_1} \wedge$

$... \wedge \varphi^{i_k}$ is a differential form and $df(p)(v_p) = Df(p)(v)$. $df = \sum_i^n D_i f dx^i$.

Results on forms: If $f : \mathbb{R}^n \to \mathbb{R}^m$, $f_* : {\mathbb{R}^n}_p \to {\mathbb{R}^m}_p$ by $f_*(v_p) = (Df(p)(v))_{f(p)}$. Thus $f_* : \Lambda^k({\mathbb{R}^m}_{f(p)}) \to \Lambda^k({\mathbb{R}^n}_p)$. So if ω is a $k-$form on $\mathbb{R}^m$, $f^*\omega(p) = f^*(\omega(p))$ is a $k-$form on $\mathbb{R}^n$. $f^*(dx^i) = \sum_j D_j f^i \cdot dx^j$, $f^*(\omega_1+\omega_2) = f^*(\omega_1)+f^*(\omega_2)$, $f^*(g\cdot\omega) = g\circ f f^*\omega$ and $f^*(\omega+\eta) = f^*\omega+f^*\eta$. If $f : \mathbb{R}^n \to R$, $Df(p) \in \Lambda^1(\mathbb{R}^n)$. $df(p)(v_p) = Df(p)(v)$. $f_*(v_p) = (Df(p)(v))_{f(p)}$. $f : \mathbb{R}^n \to \mathbb{R}^m$, $f_* : {\mathbb{R}^n}_p \to {\mathbb{R}^m}_{f(p)}$. $f_* : \Lambda^k({\mathbb{R}^m}_{f(p)}) \to \Lambda^k({\mathbb{R}^n}_p)$. $f^*(dx^i) = \sum_{j=1}^n D_j f^i dx^j$. $f^*(g \circ \omega) = g \circ f \circ f^*\omega$. *Example:* Suppose $\omega = f_1 dx_1 + f_2 dx_2 + f_3 dx_3$ then $d\omega = (\nabla f_1) \cdot (dx_1, dx_2, dx_3) \wedge dx_1 + (\nabla \cdot f_2)(dx_1, dx_2, dx_3) \wedge dx_2 + (\nabla \cdot f_3)(dx_1, dx_2, dx_3) \wedge dx_3$.

Definitions: ω is a *closed form* if $d\omega = 0$. ω is an *exact form* if $\exists \eta : d\eta = \omega$. Note that $d^2\omega = 0$.

Poincare: If $A^{open} \subseteq \mathbb{R}^n$ is a star shaped region then every closed form in A is exact. $\partial I^n = \sum_{i=1}^n \sum_{\alpha=0,1} (-1)^{i+\alpha} {I^n}_{(i,\alpha)}$ where ${I^n}_{(i,\alpha)} = I^n(x^1, ..., , x^{i-1}, \alpha, x^{i+1}, ...x^n)$. Note that $\partial^2 I^n = 0$. If $A^{open} \subseteq \mathbb{R}^n$ and $g : A \to \mathbb{R}^p$ is differentiable and $g'(x)$ has rank p whenever $g(x) = 0$ then $g^{-1}(0)$ is an $n - p$ dimensional manifold. An n-dimensional differentiable manifold is called *orientable* if it has a differential form ω of degree n which is nonzero at every point on the manifold.

Lagrange Multipliers: Maximize $F(\vec{x})$ subject to $\phi_1(\vec{x}) = 0, \phi_2(\vec{x}) = 0, \ldots, \phi_m(\vec{x}) = 0$; form $G(\vec{x}) = F(\vec{x}) + \lambda_1\phi_1(\vec{x}) + \lambda_2\phi_2(\vec{x}) + \ldots + \lambda_m\phi_m(\vec{x})$ and solve $\frac{\partial G}{\partial x_j} = 0$. Motivation: all curves, $s(t)$ that satisfy constraints must satisfy $\nabla\phi_j(s(t)) \cdot \dot{s}(t) = 0$. Similarly, if $s(t)$ is a curve, $\frac{df(s(t))}{dt} = 0 = \nabla f(s(t)) \cdot \dot{s}(t)$.

Vectors: (a) If $\nabla \times f = 0$, $f = \nabla g$. (b) If $\nabla \cdot f = 0$, $f = \nabla \times g$.

Proof of a: Put $g(x, y, z) = \int_{x_0}^x f_1(x, y, z)$, $\partial_x g = f_1$ by fundamental theorem of calculus. $\partial_y g = \partial_y \int_{x_0}^x f_1(x, y, z) = \int_{x_0}^x \partial_y f_1(x, y, z) = \int_{x_0}^x \partial_x f_2(x, y, z) = f_2$, etc.
Proof of b: Put $g_1(x, y, z) = 0$, $g_2(x, y, z) = \int_{x_0}^x f_3(t, y, z)dt - \int_{z_0}^z f_1(x_0, y, u)du$, $g_3(x, y, z) = -\int_{x_0}^x f_2(t, y, z)dt$. Using the fact that $\nabla \cdot (f_1, f_2, f_3) = 0$, we get $\nabla \times (g_1, g_2, g_3) = (f_1, f_2, f_3)$.

Change of variables: Let $\vec{x} = (x_1, x_2, \ldots, x_n)$. Suppose $\mathcal{R} \subseteq \mathbb{R}^n$ $\mathcal{R}' \subseteq \mathbb{R}^n$ and the bijection $f : \mathcal{R} \to \mathcal{R}'$ is continuously differentiable then $\int_{\mathcal{R}'} F(\vec{x})d\vec{x} = \int_{\mathcal{R}} F(f(\vec{u}))|J_f(\vec{u})|d\vec{u}$ where $J_f(\vec{u}) = |det(f')|$.

Singular cube and boundaries: Given a singular cube $I^n(x_1, \ldots, x_n)$, the boundary of I^n is $\partial I^n = \sum_{j=1}^n \sum_{\alpha=0,1} I^n_{[j,\alpha]}$ where ${}^n_{[j,\alpha]} = I^n(x_1, \ldots, x_{j-1}, \alpha, x_j, \ldots, x_{n-1})$.

Green: If C surrounds $\mathcal{R}$, a simply connected region of the plane then $\int_C Pdx + Qdy = \int_{\mathcal{R}} (\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y})dxdy$.

Proof: Just apply Fubini with bounding curves.

Gauss: If $\mathcal{S}$ is a surface enclosing a convex region $\mathcal{V}$ and $\vec{F}$ is continuously differentiable then $\int_{\mathcal{V}} \nabla \cdot \vec{F}(\vec{x})d\vec{x} = \int_{\vec{S}} \vec{F}(\vec{x}) \cdot dS$.

Proof: Apply Fubini and the Fundamental Theorem of Calculus.

Stokes: If $\mathcal{S}$ with boundary $\mathcal{C}$ and $\vec{F}$ is continuously differentiable then $\int_{\mathcal{S}} \nabla \times \vec{F}(\vec{x}) \cdot dS = \int_{\vec{C}} \vec{F}(\vec{x}) \cdot d\vec{l}$.

Proof: Apply Fubini and the Fundamental Theorem of Calculus.

Modern formulation of Stokes: If M is a compact oriented $k-$dimensional manifold with boundary and ω is a $k-1$ form on M then $\int_c d\omega = \int_{\partial c} \omega$.

Fourier: $F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(u)e^{iux}du$ and $f(u) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} F(x)e^{-iux}dx$.

Proof: First show that if $\psi(t)$ is bounded and continuous on (a,b) then $\lim_{A\to\infty}\int_a^b \psi(t)sin(At)dt = 0$. Look at $I_A = \frac{1}{\pi}\int_0^A d\tau \int_{-\infty}^{\infty} dt f(t)cos(\tau(t-x))$. Also note that $\int_0^\infty \frac{sin(At)}{t}dt = \frac{\pi}{2}$

Fourier: Let $f(x)$ be defined for $-L \le x \le L$ with $f(x+2L) = f(x)$ then $f(x) = \frac{a_0}{2} + \sum_{n=1}^{\infty}(a_n cos(\frac{n\pi x}{L}) + b_n sin(\frac{n\pi x}{L}))$ with $a_n = \int_{-L}^{L} f(x)cos(\frac{n\pi x}{L})dx$ and $b_n = \int_{-L}^{L} f(x)sin(\frac{n\pi x}{L})dx$. Parseval: $\int_{-L}^{L} f(x)^2 = \frac{{a_0}^2}{2} + \sum_{n=1}^{\infty} {a_n}^2 + {b_n}^2$. If $F(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty} f(u)e^{iux}du$, $\int_{-\infty}^{\infty} F(\alpha)G(\alpha)e^{i\alpha u}du = \int_{-\infty}^{\infty} f(u)g(x-u)du$.

Calculus of variations: Let $I = \int_{x_1}^{x_2} L(x,y,y')dx$ and $f(x)$ be the function that minimizes I ($\delta I = 0$), then $-\frac{d}{dx}\frac{\partial L}{\partial y'} + \frac{\partial L}{\partial y} = 0$.

Proof: Let $\eta(x)$ be a small functional variation with $\eta(x_1) = \eta(x_2) = 0$. $\delta I = \int_{x_1}^{x_2} L(x, y+\eta, y' + \eta')dx - \int_{x_1}^{x_2} L(x,y,y')dx$. $\delta I = \int_{x_1}^{x_2}(\frac{\partial L(x,y,y'+\eta')}{\partial y}\eta(x) + \frac{\partial L(x,y,y')}{\partial y'}\eta(x)')dx$. Integrating by parts and using $\eta(x_1) = \eta(x_2) = 0$, $\delta I = \int_{x_1}^{x_2}(\frac{\partial L(x,y,y')}{\partial y} - \frac{d}{dx}\frac{\partial L(x,y,y')}{\partial y'})\eta(x)dx$. Since $\delta I = 0$ and η was arbitrary, $\frac{\partial L(x,y,y')}{\partial y} - \frac{d}{dx}\frac{\partial L(x,y,y')}{\partial y'} = 0$. This is the Euler-Lagrange equation. In physics, $L = KE - PE$.

1.3.3 Complex Analysis

Stereographic projection: Let $S = \{(x_1,x_2,x_3) \in \mathbb{R}^3 : x_1^2 + x_2^2 + x_3^2 = 1\}$. Consider the bijective correspondence $S - \{(0,0,1)\} \leftrightarrow \mathbb{C}$ given by $(x_1,x_2,x_3) \mapsto \frac{x_1+ix_2}{1-x_3}$. S is called the *Riemann sphere* and $(0,0,1) \mapsto \infty$. $x_1 = \frac{z+\overline{z}}{1+|z|^2}$, $x_3 = \frac{z-\overline{z}}{1+|z|^2}$

Theorem: If all zeros of $P \in \mathbb{C}[z]$ lie in a half plane so do the zeros of $P'(z)$.

Theorem: If $R(z) = \frac{a_0+a_1z+a_2z^2+\ldots+a_nz^n}{b_0+b_1z+b_2z^2+\ldots+b_mz^m}$, the number of poles is $max(m,n)$ and so is the number of zeros; the common value is called the order of R.

Theorem: If $f(z) = a_0 + a_1z + a_2z^2 + \ldots + a_nz^n + \ldots$, the *radius of convergence* is R. The function is analytic if $|Z| < R$ and $\frac{1}{R} = \limsup_{n\to\infty}|a_n|^{1/n}$.

Theorem: If $a_0 + a_1 + a_2 + \ldots + a_n + \ldots$ converges then $f(z) = a_0 + a_1z + a_2z^2 + \ldots + a_nz^n + \ldots$ tends to $f(1)$ as $z \to 1$ and $\frac{|1-z|}{1-|z|}$ remains unbounded.

Theorem: A cross-ratio is real iff all four points lie on a circle or a straight line.

Definition: A function is *analytic* in Ω if it is differentiable. A function that is analytic on all of $\mathbb{C}$ is called *entire*. A function that is analytic on all of $\mathbb{C}$ except at a finite number of poles is called *meromorphic*. Over $\mathbb{C}$, the unimodular transformations are of the form $z \mapsto \frac{az+b}{cz+d}$. $log(w) = log(|w|) + iarg(w)$.

Definition: $Im(\frac{z-a}{b}) < 0$ is a *half-plane*. A set is connected if it cannot be be written as a union of non-empty disjoint open sets. A space is *Hausdorff* if $\forall x, y$ there are open subsets O_1, O_2 such that $x \in O_1, y \notin O_1$ and $y \in O_2, x \notin O_2$. A *region* is a connected open set.

Theorem: If $f(x+iy) = u(x,y) + iv(x,y)$ is analytic in a region $\mathcal{R}$ then $\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}$ and $\frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}$.

Proof: $f'(z) = lim_{\Delta x\to 0}\frac{u(x+\Delta x,y)-u(x,y)}{\Delta x} + i\frac{v(x+\Delta x,y)-v(x,y)}{\Delta x} = \frac{\partial u}{\partial x} + i\frac{\partial v}{\partial x}$. Similarly, $f'(z) = lim_{\Delta y\to 0}\frac{u(x,y+\Delta y)-u(x,y)}{i\Delta y} + i\frac{v(x,y+\Delta y)-v(x,y)}{i\Delta y} = -i\frac{\partial u}{\partial y} + \frac{\partial v}{\partial y}$.

Cauchy's Theorem: If $f(z)$ is analytic in a region $\mathcal{R}$ and its boundary is $\mathcal{C}$ then $\int_{\mathcal{C}} f(z)dz = 0$.

Proof: Let $f(x+yi) = u(x,y)+iv(x,y)$. $\int_{\mathcal{C}}(u+vi)(dx+idy) = \int_{\mathcal{C}}(udx-vdy)+i(vdx+udy)$. By Green's theorem, $\int_{\mathcal{C}}(udx-vdy)+i(vdx+udy) = \int\int_{\mathcal{R}}[(\frac{\partial(-v)}{\partial x} - \frac{\partial u}{\partial y}) + i(\frac{\partial(u)}{\partial x} - \frac{\partial v}{\partial y})]dxdy$. Each parenthesized term is 0 by the previous theorem.

Theorem: The line integral $\int_\gamma p\,dx + q\,dy$ in Ω depends only on the endpoints iff $\exists U : p = \frac{\partial U}{\partial x}, q = \frac{\partial U}{\partial y}$.

Proof: $\leftarrow$: $\int_{\gamma(t),a\le t\le b} p\cdot dx + q\cdot dy = \int_a^b \frac{dU}{dt}dt = U(\gamma(b)) - U(\gamma(a))$. $\rightarrow$: Define $U(x,y) = \int_{(\alpha,\beta)}^{(x,y)} p\cdot dx + q\cdot dy$, which is well defined since the integral only depends on endpoints. $p = \frac{\partial U}{\partial x}$ and $q = \frac{\partial U}{\partial y}$.

Theorem: If f is analytic in and on $R - \{a_1,\ldots,a_k\}$, where $\lim_{z\to a_i} f(z)(z-z_i) = 0$ then $\int_{\partial R} f(z) = 0$

Definition: If γ is a closed curve containing a, define $n(\gamma,a) = \frac{1}{2\pi i}\int_\gamma \frac{dz}{z-a}$.

Theorem: If f is analytic and γ is a closed curve containing a, $f(a) = \frac{1}{2\pi i n(\gamma,a)}\int_\gamma \frac{f(z)}{z-a}dz$.

Proof: Put $z = a+re^{i\theta}$ and perform the integrations with r small. Now apply Cauchy's theorem in the annular region when r is large.

Theorem: If φ is continuous on γ then $F_n(z) = \int_\gamma \frac{\varphi(w)}{(w-z)^n}dw$ is analytic and $F_n'(z) = nF_{n+1}(z)$.

Theorem: If $f(z)$ is analytic inside and on a circle $\mathcal{C}$ of radius r and center at $z = a$ then $f(a) = \frac{1}{2\pi}\int_0^{2\pi} f(a+re^{i\theta})d\theta$.

Proof: Because f is analytic, $\frac{1}{2\pi}\int_0^{2\pi} f(a+r_1e^{i\theta})d\theta = \frac{1}{2\pi}\int_0^{2\pi} f(a+r_2e^{i\theta})d\theta$ if $r_1, r_2 > 0$; so by continuity, $\frac{1}{2\pi}\int_0^{2\pi} f(a+r_1e^{i\theta})d\theta = lim_{r\to 0}\frac{1}{2\pi}\int_0^{2\pi} f(a+r_1e^{i\theta})d\theta = f(a)$.

Cauchy Integral Formula: If $f(z)$ is analytic inside and on a closed curve $\mathcal{C}$ and a is any point inside $\mathcal{C}$ then $f^{(n)}(a) = \frac{1}{2\pi i}\int_{\mathcal{C}} \frac{f(z)}{(z-a)^{n+1}}dz$.

Proof: By induction. For $n = 0$, put $z = a+re^{i\theta}$ then $\frac{1}{2\pi i}\int_{\mathcal{C}} \frac{f(z)}{(z-a)}dz = \frac{1}{2\pi i}\int_0^{2\pi} if(a+re^{i\theta})d\theta = f(a)$. Now by the $n = 0$ result, $\frac{g(a+h)-g(a)}{h} = \frac{1}{2\pi i h}\int_{\mathcal{C}}(\frac{g(z)}{(z-a-h)} - \frac{g(z)}{(z-a)})dz = \frac{1}{2\pi i}\int_{\mathcal{C}} \frac{g(z)}{(z-a)(z-a-h)}dz$ provided $\mathcal{C}$ encloses both a and $a+h$. Taking the limit as $h\to 0$, we get $g'(a) = \frac{1}{2\pi i}\int_{\mathcal{C}} \frac{g(z)}{(z-a)^2}dz$ and the result follows by induction.

Morrera's Theorem: If $f(z)$ is continuous in a simply connected region $\mathcal{R}$ and $\int_{\mathcal{C}} f(z)dz = 0$ around every simple closed curve $\mathcal{C}$ in $\mathcal{R}$, then $f(z)$ is analytic in $\mathcal{R}$.

Proof: By contunuity, the integral exists and by Cauchy's integral formula, the derivative exists.

Theorem: If $f(z)$ is analytic inside and on a circle $\mathcal{C}$ of radius r and center at $z = a$ then $|f^{(n)}(a)| \le \frac{M}{r^n}$ where $|f(z)| \le M$ on $\mathcal{C}$ in $\mathcal{R}$. If an analytic function is bounded in the plane it is constant. If a_n is the coefficient of z^n in the Taylor expansion of $f(z)$ about a, and f is bounded as above, $|a_n| = |\frac{f^{(n)}(a)}{n!}| \le \frac{Mn!}{r^n}$.

Proof: Let $\mathcal{C}(r)$ be a circle of radius r then by Cauchy's integral formula, $f^{(n)}(a) = \frac{1}{2\pi i}\int_{\mathcal{C}(r)} \frac{f(z)}{(z-a)^{n+1}}dz = \frac{1}{2\pi i}\int_0^{2\pi} \frac{f(a+re^{i\theta})}{(re^{i\theta})^{n+1}} re^{i\theta} d\theta$. So $|f^{(n)}(a)| = \frac{|M|}{r^n}$. The two subsequent statements follow easily.

Theorem: If $f(z)$ is analytic inside and on a closed curve $\mathcal{C}$ except at a finite number of pole then $\frac{1}{2\pi i}\int_{\mathcal{C}} \frac{f'(z)}{f(z)} = N - P$ where N and P are, respectively, the number of zeros and poles of $f(z)$ inside $\mathcal{C}$.

Proof: Let $f(z) = p(z)g(z)$ so $f'(z) = p'(z)g(z) + p(z)g'(z)$. Thus $\int_{\mathcal{C}} \frac{f'(z)}{f(z)}dz = \int_{\mathcal{C}} \frac{p'(z)}{p(z)} + \frac{g'(z)}{g(z)}dz$. So by induction, it suffices to consider $p(z) = (z-a)$ and $p(z) = (z-a)^{-1}$. In the first case, setting $z = re^{i\theta}$ $\int_{\mathcal{C}} \frac{p'(z)}{p(z)}dz = \int_{\mathcal{C}} \frac{1}{(z-a)}dz = \frac{1}{2\pi i}\int_0^{2\pi} id\theta = 1$ and in the second case, again setting $z = re^{i\theta}$ $\int_{\mathcal{C}} \frac{p'(z)}{p(z)}dz = \int_{\mathcal{C}} \frac{-1}{(z-a)}dz = \frac{-1}{2\pi i}\int_0^{2\pi} id\theta = -1$.

Theorem: If $f(z)$ is analytic in and on a ball centered at a of radius r, $B_r(a)$, then $|f^{(n)}(a)| \leq \frac{Mn!}{r^n}$, where $|f(z)| \leq M, z \in B_r(a)$.

Proof: Use the Cauchy integral formula.

Theorem: If $f(z)$ is bounded and analytic in the plane, $f(z)$ is a constant.

Proof: $f(b) - f(a) = \frac{b-a}{2\pi i}\int_{B_r(a)} \frac{f(z)}{(z-a)(z-b)}dz$. So $|f(b) - f(a)| \leq \frac{2|b-a|M}{r}$; let $r \to \infty$.

Rouche's Theorem: If $f(z), g(z)$ are analytic in and on a simple closed curve C and $|f(z)| > |g(z)|$ on C then $f(z)$ and $f(z) + g(z)$ have the same number of zeros in C.

Proof: Let $g(z) = F(z)f(z)$ so $|F(z)| < 1$. $\Delta N = \frac{1}{2\pi i}\int_{\mathcal{C}} \frac{f'(z)+g'(z)}{f(z)+g(z)}dz - \frac{1}{2\pi i}\int_{\mathcal{C}} \frac{f'(z)}{f(z)}dz = \frac{1}{2\pi i}\int_{\mathcal{C}} \frac{f'(z)+F'(z)f(z)+F(z)f'(z))}{f(z)(1+F(z))}dz - \frac{1}{2\pi i}\int_{\mathcal{C}} \frac{f'(z)}{f(z)}dz = \frac{1}{2\pi i}\int_{\mathcal{C}} \frac{F'(z)}{(1+F(z))}dz$. Since $|F(z)| < 1$, $(1 + F(z))(1 - F(z) + F^2(z) - F^3(z) + \ldots$, $\Delta N = \frac{1}{2\pi i}\int_{\mathcal{C}} \frac{F'(z)}{(1+F(z))}dz = \frac{1}{2\pi i}\int_{\mathcal{C}} F'(z)(1 - F(z) + F^2(z) - \ldots)dz = \frac{1}{2\pi i}\int_{\mathcal{C}} F'(z)dz - \frac{1}{2\pi i}\int_{\mathcal{C}} F'(z)F(z)dz + \frac{1}{2\pi i}\int_{\mathcal{C}} F'(z)F^2(z)dz - \ldots$ and each of these integrals is 0. Thus $\Delta N = 0$ and the theorem holds by the previous result.

Definition: A complex function, $f(z)$, is *holomorphic* if it is differentiable everywhere on $\mathbb{C}$. A complex function, $f(z)$, has a *removeable singularity* at a if $f(a)$ is undefined but there is a choice $b = f(a)$ which makes f holomorphic. A complex function, $f(z)$, has an *essential singularity* at a if $f(a)$ is neither a pole nor a removeable singularity.

Theorem: An analytic function comes arbitrarily close to any value in $\mathbb{C}$ in every neighborhood of an essential singularity.

Maximum Modulus Theorem: If $f(z)$ is analytic inside and on a region enclosed by a curve $\mathcal{C}$ then the point with maximum modulus lies on $\mathcal{C}$.

Proof: Suppose $|f|$ achieved its maximum at a inside $\mathcal{C}$ and $f(a) = M$. If f is not constant, we can choose a $B_r(a)$ for which $|f(x)| < M$ for some $x \in B_r(a)$. $\frac{1}{2\pi i}\int_{B_r(a)} \frac{f(z)}{z-a}dz = f(a) = M$ $\frac{1}{2\pi}|\int_{B_r(a)} \frac{f(z)}{z-a}dz| = |f(a)| = M$. So, $\frac{1}{2\pi}\int_0^{2\pi} |\frac{f(z)}{z-a}dz| \geq M$. This is impossible, since $|f(x)| < M$ for some x.

Laurent's Theorem: If $f(z)$ is analytic inside an annular region (but not necessarily in the whole disk) $\mathcal{A} = \{r \leq z - a \leq R\}$ then $f(z) = \sum_{n=-\infty}^{\infty} c_n(z-a)^n$ and $c_n = \frac{1}{2\pi i}\int_{\mathcal{C}(R)} \frac{f(z)}{(z-a)^{n+1}}dz, n \geq 0$ while $c_n = \frac{1}{2\pi i}\int_{\mathcal{C}(r)} f(z)(z-a)^{n-1}dz, n < 0$.

Proof: By Cauchy, $f(z) = \frac{1}{2\pi i}\int_{\mathcal{C}(R)} \frac{f(w)}{w-z}dz - \frac{1}{2\pi i}\int_{\mathcal{C}(r)} \frac{f(w)}{w-z}dz$. $\frac{1}{w-z} = \frac{1}{w-a} + \frac{(z-a)}{(w-a)^2} + \frac{(z-a)^2}{(w-a)^3} + \ldots + \frac{(z-a)^n}{(w-a)^n}\frac{1}{w-z}$ and $-\frac{1}{w-z} = \frac{1}{z-a}(1 + \frac{(w-a)}{(z-a)} + (\frac{(w-a)}{(z-a)})^2 + \ldots + (\frac{(w-a)}{(z-a)})^{n-1}) + (\frac{(w-a)}{(z-a)})^n\frac{1}{z-w}$. Further, $|\frac{w-a}{z-a}| = \kappa < 1$. So $\frac{1}{2\pi i}\int_{\mathcal{C}(R)} \frac{f(w)}{w-z}dw = \frac{1}{2\pi i}\int_{\mathcal{C}(R)} \frac{f(w)}{w-a}dw + \frac{z-a}{2\pi i}\int_{\mathcal{C}(R)} \frac{f(w)}{w-a}dw + \frac{(z-a)^2}{2\pi i}\int_{\mathcal{C}(R)} \frac{f(w)}{(w-a)^2}dw + \ldots + \frac{(z-a)^n}{2\pi i}\int_{\mathcal{C}(R)} \frac{f(w)}{(w-a)^n}dw + U_n$ where $U_n = \frac{1}{2\pi i}\int_{\mathcal{C}(R)}(\frac{z-a}{w-a})^n \frac{f(w)}{(w-z)}dw$ and $-\frac{1}{2\pi i}\int_{\mathcal{C}(r)} \frac{f(w)}{w-z}dw = \frac{1}{2\pi i}\int_{\mathcal{C}(r)} \frac{f(w)}{z-a}dw + \frac{1}{2\pi i}\int_{\mathcal{C}(r)} f(w)\frac{(w-a)}{(z-a)^2} + \frac{1}{2\pi i}\int_{\mathcal{C}(r)} f(w)\frac{(w-a)^2}{(z-a)^3} + \ldots + \frac{1}{2\pi i}\int_{\mathcal{C}(r)} f(w)\frac{(w-a)^{n-1}}{(z-a)^n} + \ldots + + V_n$ where $V_n = \frac{1}{2\pi i}\int_{\mathcal{C}(r)}(\frac{w-a}{z-a})^n \frac{f(w)}{(z-w)}dw$. $|U_n| \leq \frac{\kappa^n MR}{R-|z-a|}$ and $|V_n| \leq \frac{\kappa^n Mr}{|z-a|-r}$.

Residue Theorem: $\int_{\mathcal{C}} f(z)dz = 2\pi i(a_{-1} + b_{-1} + ...)$.

1.4 Probability

1.4.1 General Probability

Definitions: $\mu_X = E(X)$, ${\sigma_X}^2 = Var[X] = E[(X - E[X])^2]$. *Covariance:* $\mu_{XY} = E((X - \mu_X)(Y - \mu_Y))$. *Correlation:* $\rho(X,Y) = \frac{E((X-\mu_X)(Y-\mu_Y))}{\sigma(X)\sigma(Y)}$. *Moment generating function:* $G(e^t) = \sum_{k\geq 0} \Pr[X = k]e^{tk} = E[e^{tX}]$. *Example:* The moment generating function for Poisson distribution ($f(x) = e^{-\lambda x}$) is $\phi(t) = E(e^{tx}) = \int_0^\infty e^{tx}\lambda e^{-\lambda x}dx = \frac{\lambda}{\lambda - t}$. $E(X^2) = \frac{d}{dt}\phi(t) = \frac{2}{\lambda^2}$. $Var(X) = \frac{1}{\lambda^2}$.

Theorem(Stirling approximation): $n! \approx \sqrt{2\pi n}(\frac{n}{e})^n$.

Proof: $M_n = ln(n!) = \sum_{i=1}^n ln(i)$. $\int_0^n ln(x)dx < M_n < \int_1^{n+1} ln(x)dx$. So $(n)ln(n) - n < M_n < (n+1)ln(n+1) - n$. Set $d_n = ln(n!) - (n + \frac{1}{2})ln(n) + n$. $d_n - d_{n+1} = (n + \frac{1}{2})ln(\frac{n+1}{n}) - 1$. Writing $\frac{n+1}{n} = \frac{1+\frac{1}{2n+1}}{1-\frac{1}{2n+1}}$, expanding the log, and comparing to the geometric series in $2n+1$, we find $d_n - d_{n+1} = \frac{1}{3(2n+1)^2} + \frac{1}{5(2n+1)^4} + \ldots < \frac{1}{3}\frac{1}{(2n+1)^2-1} = \frac{1}{12}(\frac{1}{n} - \frac{1}{n+1})$. So, $0 < d_n - d_{n+1} < \frac{1}{12n} - \frac{1}{12(n+1)}$ and $\langle d_n \rangle$ is decreasing while $\langle d_n - \frac{1}{12n} \rangle$ is increasing. Thus, d_n converges to, say, C. So, $n! \approx e^C n^{n+\frac{1}{2}} e^{-n}$. To find $e^C = \sqrt{2\pi}$, use Wallis' formula: $lim_{n\to\infty} \frac{(n!)^2 2^{2n}}{(2n)!\sqrt{n}} = \sqrt{\pi}$. To get this, show $\int_0^{\frac{\pi}{2}} sin^n(x) = \frac{n-1}{n}\int_0^{\frac{\pi}{2}} sin^{n-2}(x)$.

Bayes Theorem: $P(B_i|A) = \frac{P(A|B_i)P(B_i)}{\sum P(A|B_j)P(B_j)}$.

Normal Distribution: $N(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$, $Z = \frac{(X-np)}{\sqrt{npq}}$.

Binomial Distribution: $B(N,n,p) = \binom{N}{n} p^n (1-p)^{N-n}$, $E(B) = Np, \sigma^2 = Np(1-p)$.

Poisson Distribution: $P(x) = e^{-\lambda}\frac{\lambda^x}{x!}$, $\mu = \lambda, \sigma^2 = \lambda$, probability of count in time Δt is $\lambda \Delta t$.

$$f(x,y) = \frac{1}{2\pi\sigma_1\sigma_2\sqrt{1-\rho^2}} e^{-(\frac{(x-\mu_1)^2}{\sigma_1^2} + (2\rho)\frac{(x-\mu_1)(y-\mu_2)}{\sigma_1\sigma_2} + \frac{(y-\mu_2)^2}{\sigma_2^2})/(2\sqrt{1-\rho^2})}$$

ρ is the cross correlation between x and y.

Poisson approximation to binomial distribution: When $p << 1$ Poisson approximates binomial with $np = \lambda$, $E(X) = \lambda$.

Binomial test: If we have an experiment with two outcomes and we want to test the hypothesis that the distribution of outcomes is $p, q = 1 - p$. We perform n experiments. We expect about np observations of the first outcome. Suppose there are r observation of the first value. The *binomial* test with significance α, tests the hypothesis that the proposed distribution is correct. To do it, let the random variable x represent the number of "successes". Compute $P(x \geq r) = \sum_{j=r}^n \binom{n}{j} p^j (1-p)^{n-j}$. If $P(x \geq r) < \alpha$, reject the hypothesis.

Zipf distribution: $P(k) = \frac{c}{k^{1+\alpha}}$.

Central Limit Theorem: If X_i are independent, identically distributed random variables with mean μ and $S_n = X_1 + \ldots + X_n$, then $\lim_{n\to\infty} P(a \leq \frac{(S_n - n\mu)}{\sigma\sqrt{n}} \leq b) = \frac{1}{\sqrt{(2\pi)}} \int_a^b e^{-(u^2/2)}$.

Proof: $E(S_n) = n\mu$, $\sigma^2 = Var(S_n) = n\sigma_{X_i}$. Define $S_n^* = \frac{S_n - n\mu}{\sigma\sqrt{n}}$. So $E[e^{tS_n^*}] = E[e^{\frac{t(X_1-\mu)}{\sigma\sqrt{n}}} e^{\frac{t(X_2-\mu)}{\sigma\sqrt{n}}} \ldots e^{\frac{t(X_n-\mu)}{\sigma\sqrt{n}}}] = E[e^{\frac{t(X_1-\mu)}{\sigma\sqrt{n}}}]^n$. Expanding the exponential in the taylor series, we get $E[e^{tS_n^*}] = E[1 + \frac{t(X-\mu)}{1!\sqrt{n}\sigma} + \frac{(t(X-\mu))^2}{2!(\sqrt{n}\sigma)^2} + \ldots]^n = e^{\frac{-t^2}{2}}$. This is the same moment generating function as the normal distribution, so were done.

$\chi^2 = \frac{(Y_2 - np_2)^2}{(np_2)} + ... + \frac{(Y_{12} - np_{12})^2}{(np_{12})}$, $P(\chi^2 \leq x) = \frac{1}{2^{\frac{\nu}{2}}\Gamma(\frac{\nu}{2})} \int_0^x u^{\frac{\nu}{2}-1} e^{-\frac{u}{2}} du$.

Markov Inequality: Let X be a random variable assuming only non-negative values, and with expected value $E[X]$ convergent. Then for any $t > 0$, $\Pr[X \geq t] \leq \frac{E[X]}{t}$.

Proof: Let $f(x)$ be the density function. Let I_E be the indicator function of the set of events E ($I_E(e) = 1$, if $e \in E$, 0 otherwise). $E(aI_{|X|\geq a}) \leq E(|X|)$, so $aPr(|X| \geq a) \leq E(|X|)$.

Chebyshev Inequality: Let Y be a random variable with expected value $\mu = E[Y]$ and variance, $Var(Y)$. Then for any $t > 0$, $\Pr[|Y - \mu| \geq t] \leq \frac{Var(Y)}{t^2}$.

Proof: Let $g(y)$ be the density function. $Var(Y) = \int_{-\infty}^{\infty}(Y - E(Y))^2 g(y)dy$. $Var(Y) \geq \int_{|Y-E(Y)|\geq\epsilon}(Y - E(Y))^2 g(y)dy \geq \epsilon^2 \int_{|Y-E(Y)|\geq\epsilon} g(y)dy = \epsilon^2 P(|Y - E(Y)| \geq \epsilon)$.

Chernoff: Let $T_1, T_2, \ldots, T_N$ be mutually independent Bernoulli variables $T = \sum_i^N T_i$. Then $\forall c \geq 0$, $Pr(T \geq cE(T)) \leq e^{\alpha E(T)}$ where $\alpha = ln(c) + \frac{1}{c} - 1$.

Wald: Let Q be a random variable that takes on only non-negative integer values such that $E(Q) < \infty$. Let $R_1, R_2, \ldots$ be a sequence of random variables with the same distribution and let $T = R_1 + R_2 + \ldots + R_Q$. Suppose R_k is independent of the event that it is included in the sum, that is $\forall k \geq 1$, R_k is independent of an indicator variable for the event $Q \geq k$ then $E(T) = E(Q)E(R_1)$.

Occupancy: Let X_i be an indicator for a ball falling into i. $E(X_i) = 1$. Let Z_i be the probability that the bin is empty. $E(Z_i) = \frac{n}{e}$. Let $p_m(r, n)$ be the probability of finding r balls in n cells with exactly m empty cells. $p_m(r, n) = \binom{n}{m}(1 - \frac{m}{n})^r p_0(r, n - m)$. Further, $p_0(r, n) = \sum_{i=0}^{n}(-1)^i \binom{n}{i}(1 - \frac{i}{n})^r$.

Lovasz Local Lemma: Let $G = (V, E)$ be a dependency graph for events $e_1, e_2, ..., e_n$ in a probability space. Suppose $\exists x_i \in [0, 1]$ for $1 \leq i \leq n$, such that $Pr[e_i] \leq x_i \Pi_{(i,j)\in E}(1 - x_j)$. Then $Pr[\cap\overline{e_i}] \geq \Pi_i^n(1 - x_i)$.

Theorem: If $\{p_i\}$ and $\{q_i\}$ are probability distributions and $G(q_1, q_2, \ldots, q_n) = -\sum p_i ln(q_i)$. Then G is minimum when $p_i = q_i$.

1.4.2 Statistical Inference and Hidden Markov Models

Sample statistics: Suppose a population has mean μ and variance σ. If we take a sample of size n consisting of observations $\langle X_1, \ldots, X_n\rangle$ and let $\mu_{\overline{X}}$ denote the sample mean, then $E((\mu_{\overline{X}} - \mu)^2) = \frac{\sigma^2}{n}$. The *chi-squared* random variable for normally distributed random variables $\langle X_1, \ldots, X_n\rangle$ with mean 0 and variance 1 is is defined as $\chi^2(\langle X_1, \ldots, X_n\rangle) = X_1^2 + \ldots + X_n^2$; $P(\chi^2 \leq x) = \frac{1}{2^{\frac{\nu}{2}}\Gamma(\frac{\nu}{2})} \int_0^x u^{\frac{\nu}{2}-1} e^{-\frac{u}{2}} du$ where ν is the number of degrees of freedom. Now let $S^2 = \frac{(X_1 - \mu_{\overline{X}})^2 + \ldots + (X_n - \mu_{\overline{X}})^2}{n}$. If the distributions are normal, the distribution of S^2 is *chi-squared* with $n - 1$ degrees of freedom. $\chi^2 = \frac{nS^2}{\sigma^2}$. Thus if H_0 is a hypothesis from a normal distribution, we accept at .05 level if $\chi^2(.025) \leq \frac{ns^2}{\sigma^2} \leq \chi^2(.975)$. Finally, put $T = \frac{\mu_{\overline{X}} - \mu}{\frac{S}{\sqrt{n-1}}}$. This is Student

t-distributed with $n-1$ degrees of freedom.

Let $Y = Pred(L)$, $\sigma^2(Y,L) = E((Y-L)^2)$. Value of predictor: $W(Y,L) = \frac{\sigma^2(Y,L)-E(L-Y)^2}{\sigma^2(Y,L)}$. $0 = W(E(L),L) \leq W(Y,L) \leq W(L,L) = 1$. $E((X-t)^2)$ is minimized $t = E(Y)$. Let $cov(X,Y) = E(XY) = E(X)E(Y)$. Best linear predictor: $Y = aX + b$, $a = \frac{cov(X,Y)}{cov(X,X)}$ (and solve for b). Worth of best predictor (using mean square error) is $\rho(X,Y)^2 = \frac{cov(X,Y)^2}{cov(X,X)cov(Y,Y)}$. Posterior models. $P(|Y-\mu| \geq t) \leq \frac{var(Y)}{t^2}$.

Maximum likelihood re-estimation: Let $S = \{1,2,3,\ldots,n\}$ be the n possible states of a hidden markov process with $T-1$ transitions and T outputs. Suppose the output vector of the process is $\vec{O} \in (\mathbb{Z}_m)^{(T)}$. Finally, suppose the following distributions are given: initial state distribution - $\pi(i), i \in \mathbb{Z}_m$; output distribution - $q_{ij} = q(j|i) = Pr(O_t = j|\vec{S}_t = i), \forall t$; state transition distribution: $p_{ij} = P(j|i) = Pr(\vec{S}_t = j|\vec{S}_{t-1} = i), \forall t$.

- *Problem 1:* Given $O = O_0, O_1, O_2, ..., O_{T-1}$, $\lambda = (P,q,\pi)$, how do we compute $Pr(O|\lambda)$ efficiently?
- *Problem 2:* Given $\vec{O} = O_0, O_1, O_2, ..., O_{T-1}$ and λ, how do we choose an $\vec{q}$ which is optimal?
- *Problem 3:* How do we adjust the model parameters $\lambda = (P,q,\pi)$, to optimize $Pr(\vec{O}|\lambda)$, given the observed sequence: $\vec{O}$?

Solution to Problem 1: Assuming the foregoing, the probability of the output $\vec{O}$ is:

$$Pr[\vec{O}|\lambda] = \sum_{\vec{s} \in \vec{S}^{(T)}} \pi(\vec{s}_0) q(O_0|\vec{s}_0) \prod_{i=1}^{T} P(\vec{s}_i|\vec{s}_{i-1}) \prod_{i=1}^{T} q(O_i|\vec{s}_i)$$

The following recursion greatly improves the calculation cost. Let $\alpha_0(i) = \pi(i)q(O_0|i), \forall i$ and $\alpha_t(i) = (\sum_{j=1}^{n} \alpha_{t-1}(j)P(S_t = i|S_{t-1} = j))q(O_t|i), \forall i$. This is called the "forward recursion". Then $\alpha_t(i) = \sum_{\vec{s} \in \vec{S}^t, \vec{s}_t = i} \pi(\vec{s}_0)q(O_0|\vec{s}_0) \prod_{j=1}^{t} P(\vec{s}_j|\vec{s}_{j-1}) \prod_{j=1}^{t} q(O_j|\vec{s}_j)$, the probability of the observation of the sequence up to time t given $\vec{s}_t = i$. $Pr(\vec{O}|\lambda) = \sum_{i=1}^{n} \alpha_{T-1}(i)$; computing $\{\alpha_T(i)\}$ takes $O(n^2(T))$ rather than $O(2(T)n^T)$. This solves problem 1.

Solution to Problem 2: Slightly abusing the notation from above define $\beta_t(i) = Pr(O_{t+1}, \ldots, O_T|S_t = i, \lambda)$. The "backwards recursion" is: $\beta_T(i) = 1, \forall i$, $\beta_t(i) = \sum_{j=1}^{n} P(S_t = i|S_{t+1} = j)\beta_{t+1}(j)q(O_{t+1}|j)$. Now define $\gamma_t(j) = P(s_t = 1|\vec{O}, \lambda)$ so $\gamma_t(j) = \frac{\alpha_t(j)\beta_t(j)}{P(\vec{O}|\lambda)}$. The most likely state at time t is the one that maximizes $\gamma_t(i)$.

Solution of Problem 3: Define $\gamma_t(i,j) = P(S_t = i, S_{t+1} = j|\vec{O}, \lambda)$ so $\gamma_t(i,j) = \frac{\alpha_t(i)P(S_t=j|S_{t+1}=i)q(O_{t+1}|j)\beta_{t+1}(j)}{P(\vec{O}|\lambda)}$ and $\gamma_t(i) = \sum_{j=1}^{n} \gamma_t(i,j)$. $\gamma_t(i,j)$ is the probability of being in state i at t and transitioning to state j. Now, suppose the model, $\lambda = (\pi, P, q)$, is unknown, the MLE of the model, given observations $\vec{O}$ is determined by:

- $0 = \frac{\partial}{\partial \pi(i)}[Pr(\vec{O} = (O_0, \ldots, O_T)) - \lambda_1(\sum_{k=0}^{m-1} \pi(k) - 1)]$.
- $0 = \frac{\partial}{\partial P(j|i)}[Pr(\vec{O} = (O_0, \ldots, O_T)) - \lambda_2(\sum_{k=0}^{m-1} P(k|i) - 1)]$.
- $0 = \frac{\partial}{\partial q(j|i)}[Pr(\vec{O} = (O_0, \ldots, O_T)) - \lambda_3(\sum_{k=0}^{m-1} q(k|i) - 1)]$.

Solving gives the following *re-estimation formulas:*

- $\hat{\pi}(i) = \gamma_0(i) = \frac{\alpha_0(i)\beta_0(i)}{\sum_{k=1}^{n}\alpha_0(k)\beta_0(k)}$, $\sum \pi(i) = 1$.
- $\hat{P}(j|i) = \frac{\sum_{t=0}^{T-1}\gamma_t(i,j)}{\sum_{t=0}^{T-1}\gamma_t(i)} = \frac{\sum_{t=0}^{T-1}\alpha_t(i)q(O_{t+1}|j)P(j|i)\beta_t(j)}{\sum_{t=0}^{T}\alpha_t(i)\beta_t(i)}$, $\sum_j P(j|i) = 1$.
- $\hat{q}(j|i) = \frac{\sum_{t\in\{0,1,\ldots,T-1\},O_t=j}\gamma_t(i)}{\sum_{t=0}^{T-1}\gamma_t(i)} = \frac{\sum_{t=0,O_t=j}^{T-1}\alpha_t(i)\beta_t(i)}{\sum_{t=1}^{T}\alpha_t(i)\beta_t(i)}$, $\sum_j q(j|i) = 1$.

Baum showed that if $Q(\lambda,\overline{\lambda}) = \sum_{s\in S} P_\lambda(O,s)log(P_{\overline{\lambda}}(O,s)$ and $Q(\lambda,\overline{\lambda}) > Q(\lambda,\lambda)$ then $P_{\overline{\lambda}}(O,s) > P_\lambda(O,s)$. Optimizing Q instead of P gives the Baum EM algorithm. Note that optimizing using dynamic programming may give a different result: $\delta_0(i) = \pi(i)q(i|O_0)$, $\delta_t(i) = max_{j\in\{1,\ldots,n\}}(\delta_{t-1}(j)p_{ji}q_{iO_t})$ since it optimizes the overall path. You can deal with underflow by taking logs or (in the HMM case) scaling in a way that maintains the re-estimation result.

Scaling: $\alpha_t(i) = \sum_{j=1}^{n}\alpha_{t-1}(j)a_{ji}b_i(o_t)$. $\tilde{\alpha}_0(i) = \alpha_0(i), 0 \le i < n$, $c_0 = (\sum_{j=0}^{n}\tilde{\alpha}_0(j))^{-1}$ and $\hat{\alpha}_0(i) = c_0\tilde{\alpha}_0(i)$. Recursively, $\tilde{\alpha}_t(i) = \sum_{j=1}^{n}\hat{\alpha}_{t-1}(j)a_{ji}b_i(o_t), 0 \le i < n$, $c_t = (\sum_{j=1}^{n}\tilde{\alpha}_0(j))^{-1}$ and $\hat{\alpha}_t(i) = c_t\tilde{\alpha}_0(i)$. Using the above, $\hat{\alpha}_t(i) = c_0c_1\ldots c_t\alpha_t(i) = \frac{\alpha_t(i)}{\sum_{j=1}^{n}\alpha_t(j)}$ and $P(O|\lambda) = (\prod_{j=0}^{T-1}c_j)^{-1}$, the β scale the same way.

EM as Gaussian mixture problem: $p(\vec{x}) = \sum_{k=1}^{K}N(\vec{x}|\vec{\mu_k},\vec{\Sigma_k})$, let $\vec{z}$ be a K dimensional random variable from the sample space all of whose components are 0 but a single one which is 1 (i.e.- $z_k = 1$) under the Gaussian model (π_k,μ_k,Σ_k). $p(\vec{x}|z_k = 1) = N(\vec{x}|\vec{\mu_k},\vec{\Sigma_k})$, $p(z_k = 1) = \pi_k$ and $p(\vec{x}) = p(\vec{x}|\vec{z})p(\vec{z})$. π_k is the prior estimate of $z_k = 1$ and $\gamma(z_k)$ is the posterior estimate. $\gamma(z_k) = p(z_k = 1|\vec{x}) = \frac{p(z_k=1)p(\vec{x}|z_k=1)}{\sum_j p(z_j=1)p(\vec{x}|z_j=1)}$. For mixing, let $\langle\vec{x_1},\ldots,\vec{x_N}\rangle$ be a sample. The log likelihood is $p(\vec{x}|\vec{\pi},\vec{\mu},\vec{\Sigma}) = \sum_{n=1}^{N}ln(\sum_{k=1}^{K}\pi_kN(\vec{x_n}|\mu_k,\Sigma_k))$ and EM maximizes this. Maximizing equations come from taking derivatives with respect to μ_k and setting them to 0 — $0 = -\sum_{n=1}^{N}\frac{\pi_kN(\vec{x_n}|\mu_k,\Sigma_k}{\sum_j\pi_jN(\vec{x_j}|\mu_j,\Sigma_j)}\cdot\Sigma_k(\vec{x_n}-\mu_k)$. The term in the denominator is $\gamma(z_{nk})$, $N_k = \sum_{n=1}^{N}\gamma(z_{n,k})$ and $\mu_k = \frac{1}{N_k}\sum_{n=1}^{N}\gamma(z_{n,k})$. Taking the derivatives with respect to Σ_k give the remaining equations (Note: $\mu_k = \frac{N_k}{N}$). An alternative (Bayesian) view is to regard $\vec{z}$ as latent, Θ as the model parameters and $ln(p(\vec{X}|\Theta)) = ln(\sum_z p(\vec{X}|\vec{Z},\Theta))$. We use this to estimate the likelihood from Θ^{old} for general Θ: $\mathcal{Q}(\Theta,\Theta^{old}) = \sum_z p(Z|X,\Theta^{old})ln(p(X,Z|\Theta))$; the "M" step corresponds to finding $\Theta^{new} = arg\ max_\Theta(\mathcal{Q}(\Theta,\Theta^{old})$.

Dichotomy problem: $\vec{x} = (x_1,x_2,\ldots,x_n)$ is observed stream generated by process with underlying model $P(0) = \theta_0$. Suppose a 0's are observed and b 1's, $P(\vec{x}|\theta) = \theta^a(1-\theta)^b$. The inverse problem in it's simplest form is choose between two sources of $\vec{x}$ with probabilities θ_0,θ_1, where $P(\theta_0) + P(\theta_1) = 1$. $P(\theta_i|\vec{x}) = \frac{P(\vec{x}|\theta_i)P(\theta_i)}{P(\vec{x})}$ and thus $P(\theta_i|\vec{x}) = \frac{\theta_i^a(1-\theta_i)^bP(\theta_i)}{P(\vec{x})}$. Note that $P(\vec{x}) = P(\vec{x}|\theta_0)P(\theta_0) + P(\vec{x}|\theta_1)P(\theta_1)$. The posterior odds ratio is $\frac{P(\theta_1|\vec{x})}{P(\theta_0|\vec{x})} = (\frac{\theta_1}{\theta_0})^a(\frac{(1-\theta_1)}{(1-\theta_0)})^b(\frac{P(\theta_1)}{P(\theta_0)})$. Let the "benefit" of guessing θ_i if the correct answer is θ_j be m_{ji} (negative if $i \ne j$). We maximixe the mean outcome by picking θ_1 iff $\frac{P(\vec{x}|\theta_1)}{P(\vec{x}|\theta_0)} \ge \frac{m_{00}-m_{01}}{m_{11}-m_{10}}$. The log posterior odds is $log(\frac{P(\theta_1|\vec{x})}{P(\theta_0|\vec{x})}) = log(\frac{P(\vec{x}|\theta_1)}{P(\vec{x}|\theta_0)}) + log(\frac{\theta_1}{\theta_0})$. What is PDF for $log(\frac{P(\theta_1|\vec{x})}{P(\theta_0|\vec{x})})$? $E_{\theta_i}(log(\frac{P(\theta_1|\vec{x})}{P(\theta_0|\vec{x})}) = n(\theta_ilog(\frac{\theta_i}{\theta_0}) + (1-\theta_i)log(\frac{1-\theta_i}{1-\theta_0})) + c$. Call $\mu = \theta_ilog(\frac{\theta_i}{\theta_0}) + (1-\theta_i)log(\frac{1-\theta_i}{1-\theta_0})$ the *s*coring or information rate. Note that this is irrelevant once $\vec{x}$ is evaluated. Given two distributions $\{p_i\}$ $\{q_i\}$, define $H(\vec{p},\vec{q}) = \sum_{j=1}^{n}p_jlog(\frac{p_i}{q_i})$. $H(\vec{p},\vec{q}) \ge 0$ and $H(\vec{p},\vec{q}) = 0$ iff $\{p_i\} = \{q_i\}$. Using a Taylor expansion if $\theta_0 \approx \theta_1 \approx \frac{1}{2}$, $H(\theta_1:\theta_0) \approx H(\theta_0:\theta_1)$. Claim: For large n, $log(\frac{P(\theta_1|\vec{x})}{P(\theta_0|\vec{x})})$ is approximately Gaussian distributed. Apply CLT: $\frac{1}{\sqrt{n}}(log(\frac{P(\theta_1|\vec{x})}{P(\theta_0|\vec{x})}) - \mu n) = \sum_{j=1}^{n}\frac{1}{\sqrt{n}}(log(\frac{P(\theta_1|\vec{x}_j)}{P(\theta_0|\vec{x}_j)}) = \mu$. μ is the scoring or information rate.

Data analysis: *k-means*: put $\mu_j = x_n$, for k random x_n. Repeat until $S_1,S_2,\ldots,S_k$ don't change.

Put x_i in the S_j where x_i is closest to μ_j. For $j = 1, \ldots, k$, $\mu_j = |S_j|^{-1} \sum_{x \in S_j} x$. *Naive Bayes for spam:* Get training set S, H of spam and ham messages. w_i, a word is i-th feature. Get P(spam) and P(ham) from training set. Calculate $P(w_1, w_2, \ldots, w_m|\text{spam})$. Now use Bayes theorem to get estimator.

Cryptographic application: Model incorrect decipherments as random stream $P(0) = P(1) = \frac{1}{2}$ while correct decipher $P(0) = \theta_1 \neq \frac{1}{2}$. For one time pad, we want to distinguish between $P(\cdot|\frac{1}{2})$ and $P(\cdot|\theta_1)$. We compute $\frac{P(\theta_1|\vec{z} \oplus \vec{y})}{P(\frac{1}{2}|\vec{z} \oplus \vec{y})}$ using prior $P(\frac{1}{2}) = \frac{K-1}{K}$ and $P(\theta_1) = \frac{1}{2}$. Consider an $l-$gram, $P(\vec{y}) = 2^{-l}$ for small l but this cannot be true for $l \approx n$. Define $L(\vec{x}) = log(\frac{P(\vec{x}|\theta_1)}{P(\vec{x}|\theta_0)})$. "Type I" errors reject θ_0 when it is correct. "Type II" errors accept θ_0 when it is incorrect.

Principal Component Analysis: Suppose $x_1, x_2, \ldots, x_N \in \mathbb{R}^D$ and we project this space onto $\langle u_1, u_2, \ldots, u_M \rangle$ where $u_k \in \mathbb{R}^D$ and $u_i u_i^T = 1$. For example, for $M = 1$, the variance of the projection is $\frac{1}{N} \sum_{n=1}^{N} (u_1^T x_n - u_1^T \overline{x}) = u_1^T S u_1$ where $\overline{x} = \frac{1}{N} \sum_{i=1}^{N} x_i$ and S is the co-variance matrix. Finding the first principal component requires us to to maximize $u_1^T S u_1$ subject to $u_1^t u_1 = 1$. Using Lagrange multipliers, this is equivalent to maximizing $f(u_1) = u_1^T S u_1 + \lambda_1(1 - u_1^T u_1)$. Taking derivative, we get $S(u_1) = \lambda_1 u_1$ with λ_1 the largest eigenvalue of S. Can also find λ_1 with EM. For general M, $u_i^T u_j = \delta_{ij}$, $\vec{x_n} = \sum_{i=1}^{D} \alpha_{ni} u_i$, $\alpha_{nj} = (x_n^T u_j)$, $x_n = \sum_{i=1}^{D} (x_i^T u_i \cdot u_i)$ and we want to minimize $J = \frac{1}{N} \sum_{n=1}^{N} ||x_n - \overline{x}||^2$ which reduces to an eigenvalue problem.

1.4.3 Information and Coding Theory

Shannon conditions for entropy: (a) continuous in probability, (b) monotonically increasing in number of messages, additive with respect to refinement: $H(\frac{1}{2}, \frac{1}{4}, \frac{1}{4}) = H(\frac{1}{2}, \frac{1}{2}) + \frac{1}{2} H(\frac{1}{2}, \frac{1}{2})$. Number of bits of information obtained in observing event that occurs with probability p is $lg(p)$. $H(P) = \sum -p_i lg(p_i)$, $lg(|X|) \geq H(X) \geq 0$. $I(X,Y) = H(X) - H(X|Y) = H(X) + H(Y) - H(X,Y)$. $H(X,Y) \leq H(X) + H(Y)$. $H(U|V) = 0$ iff $U = g(V)$.

Notation: $D(p||q) = \sum_x p(x) lg(\frac{p(x)}{q(x)}) \geq 0$. Markov chain denoted by $X \to Y \to Z$. If $X \to Y \to Z$ then $I(X;Y) \leq I(X;Z)$. Let $T(X)$ be any statistic and $F = \langle f_\theta(x) \rangle$ and X a sample from F then $I(\theta; T(X)) \leq I(\theta; X)$. T is a **sufficient statistic** if equality holds. $T(X)$ is a minimal sufficient statistic relative to F if it is a statistic of every other sufficient statistic $U(X)$. $\theta \to T(X) \to U(X) \to X$. A stochastic process $X = \langle X_1, X_2, \ldots \rangle$ is **stationary** if the joint distribution of any subsequence is invariant with respect to time shifts. The *entropy* of a stochastic process is $H(X) = \lim_{n \to \infty} \frac{1}{n} H(X_1, X_2, \ldots, X_n)$. For a stationary Markov chain, the entropy rate is given by $H(X) = H(X_2|X_1)$. If X is a stationary markov chain then so is the process $\langle Y_i = \phi(X_i) \rangle$ and $H(Y_n|Y_{n-1}, \ldots, Y_1, X_1) \leq H(Y) \leq H(Y_n|Y_{n-1}, \ldots, Y_1)$ equality holds by taking the limit across the inequalities.

Theorem on Asymptotic Equipartition: $H_\delta(X) = lg(min\{|T| : T \subseteq A_X, Pr(x \in T) \geq (1 - \delta)\}$ and n, independent identically distributed random variables X_i, if $X^n = (X_1, X_2, \ldots, X_n)$ is almost certain to belong to $B \subseteq A_X^n$ having about 2^{NH} members, each with probability "close" to 2^{-NH}. This is equivalent to **Shannon's Source coding Theorem:** The n r.v.'s can be encoded by NH bits with negligible information loss. To show this, show for any δ there's an n such that $H_\delta(X^{(n)}) \approx NH$. Hint: Define $Y = \frac{1}{n} lg(\frac{1}{p(x)})$. Let $T_{n,\beta} = \{y \in A_X^n : [\frac{1}{n} lg(\frac{1}{p(x)}) - H]^2 < \beta^2\}$.

Definition: The *channel capacity* is $C = max_{P(x)}(H(I|J) - H(I))$. For a DMC, BSC with error rate p, this implies $C_{BSC}(p) = 1 + plg(p) + qlg(q)$. So for BSC $R = 1 - H(P)$.

Observations: To *detect* t errors $d(C) \geq t+1$. To *correct* t errors $d(C) \geq 2t+1$. A *perfect code* satisfies $M(\sum_k^t \binom{n}{k}(q-1)^k) = q^n$.

Shannon Source Coding: If a memoryless source has entropy H then any uniquely decipherable code over an alphabet Σ with D symbols must have length $\geq \frac{H}{lg(D)}$. Further, $\exists$ a uniquely decipherable code with average length $\leq 1 + \frac{H}{lg(D)}$.

Shannon's Theorem Channel Coding: If $0 \leq R \leq 1+plg(p)+qlg(q)$, $M_n = 2^{\lceil Rn \rceil}$, then $P^*(M_n, n, p) \to 0$ as $n \to \infty$. Notation: Each codeword has n bits. Let P_i be the probability of making an error in decoding if x_i is transmitted. Then $P_C = \frac{1}{M}\sum_i P_i$ is the probability of making a decoding error if a randomly chosen codeword is transmitted and every codeword is equiprobable. $P^*(M_n, n, p) = min_C(P_C)$, with $BlockLength(C) = n$, $R = \frac{lg(|C|)}{n}$ and $M_n = 2^{\lfloor Rn \rfloor}$.

Proof: Define the following terms: $f(u,v) = 0$, if $d(u,x) > \rho$ and $f(u,v) = 1$, if $d(u,x) \leq \rho$, $g_i(y) = 1 - f(y,x_i) + \sum_{i \neq j} f(y,x_i)$. Then $P_i = \sum_y P(y|x_i)g_i(y) = \sum_y P(y|x_i)[1-f(y,x_i)] + \sum_y \sum_{i \neq j} P(y|x_i)f(y,x_i)$. So, $P_C = min_C[\frac{1}{M}\sum_i(\sum_y \sum_y P(y|x_i)[1-f(y,x_i)] + \sum_y \sum_{i \neq j} P(y|x_i)f(y,x_i))]$. Now, taking expectations over all eligible C and using the fact that at least one particular C must have $P_C \leq$ the expected value of P_C over all C, we get $P_C \leq [\frac{1}{M}\sum_i \sum_y E(P(y|x_i)[1 - f(y,x_i)]) + \sum_y \sum_{i \neq j} E(P(y|x_i))E(f(y,x_i))]$. Now, let N_e be the number of received bits in error in a string of length n, then $E(N_e) = np$ and $Var(N_e) = \sqrt{npq}$. Set $b = \sqrt{\frac{npq}{\frac{\epsilon}{2}}}$ then $P(n_e > np + b) \leq \frac{\epsilon}{2}$ by Chebychev. If $B_\rho(x)$ is the set of words of distance $\leq \rho$. So, we get $P_C \leq \frac{\epsilon}{2} + M^{-1}\sum_i \sum_y \sum_{i \neq j} E(P(y|x_i))E(f(y,x_i)) \leq \frac{\epsilon}{2} + (M-1)2^{-n}|B_\rho)|$. Now $\rho = pn$ and $B_\rho(x) = \sum_{i \leq \rho}\binom{n}{i}$. But $1 = [\lambda + (1-\lambda)]^n = \sum_{k=0}^{pn}\binom{n}{k} \leq \lambda^{pn}(1-\lambda)^{n(1-p)}\sum_{k=0}^{pn}\binom{n}{k}$. So, $2^{-nH(p)} \geq \sum_{k=0}^{pn}\binom{n}{k}$. Putting this back in the equation for P_C we get $P_C \leq \frac{\epsilon}{2} + (M-1)2^{-n(1+H(p))} \leq 2^{n(R-1-H(p))}$ which goes to 0 if $R < 1 + H(p)$.

Definitions: (n, M, d) *codes* M is number of codewords, d is minimum distance, n is dimension. An $[n,k,d]$ *linear code* is an $k-$subspace of an $n-$ space over F with minimum distance d. The *standard form for a generator* is $G = (I_k|A)$ with k message bits, n codeword bits. Codeword $c = mG$ and $d = min_{u \neq 0, u \in C}\{wt(u)\}$. The *parity check matrix*, H, of a code is the generator of its dual code. $C^\perp = \{x : (x,y))) = 0, \forall y \in C\}$. Note that $GH = 0$. If C is a code, $C^\perp$ is a code (the *dual code*). $H = (-A^T, I_{n-k})$, $GH^T = 0$. Consider a table with the codewords forming the first row, subsequent rows add error e until all 2^n blocks are in the table. Each row is a coset and the element of minimum weight in each row is called the coset leader. To decode received word $r = c + e$: (1) compute syndrome $s(r) = rH^T$, (2) find coset leader with $s(r)$ and locate the codeword, c_0 in that column, (3) decode as $r - c_0$.

Define $V(n,r) = \sum_{j=1}^r \binom{n}{j}$. **Hamming Bound:** $|C| \leq \frac{2^n}{V(n,e)}$. **Sphere Packing Bound:** If $d = 2e+1$, $A_q(n,d)\sum_{k=0}^e \binom{n}{k}(q-1)^k \leq q^n$. **GSV Bound:** $A(n,d) \geq \frac{2^n}{V(n,d-1)}$, where $A(n,d)$ is the largest code with minimum distance d.

Hamming Codes: A *Hamming code* is a $[n,k,d]$ linear code with $n = 2^m - 1$, $k = 2^m - 1 - m$ and $d = 3$. To decode, if $r = c + e$ is received (1) calculate $s(r) = rH^T$, (2) find j which is the column of H with

syndrome $s(r)$, correct position j. The $[7,4]$ code has encoding matrix

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

with check equations $y_1 + y_3 + y_5 + y_6 = 0$, $y_2 + y_3 + y_6 + y_7 = 0$, $y_4 + y_5 + y_6 + y_7 = 0$. For Hamming, $n = 2^m - 1$, m parity checks identify error position. Motivation for BCH is to use another m parity checks which identify $f(j) = j^3$ positions. Rows of Hadamard matrix $HH^T = nI$ forms a $(n, 2n, \frac{n}{2})$ code. Let A_i be the number of codewords of weight i for a code C, then $A(z) = \sum_i A_i z^i$ is the weight enumerator.

Cyclic Codes: A *cyclic code, C*, has the property that $(c_1, c_2, \ldots, c_n) \in C \rightarrow (c_n, c_1, \ldots, c_{n-1}) \in C$. Denoting $U_n(x) = x^n - 1$ we have the following theorem: C is a cyclic code of length n iff its generator $g(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \mid U_n(x)$ where codewords $c(x)$ have the form $m(x)g(x)$. Further, if $U_n(x) = h(x)g(x)$, $c(x) \in C$ iff $h(x)c(x) = 0 \,(\text{mod } U_n(x))$. *Example:* $g(x) = 1 + x^2 + x^3$ generates $(7,4)$ code. $g(x)m(x) = c(x)$, $a = (1010), a(x) = 1 + x^2$; $g(x)a(x) = c(x) = x^5 + x^4 + x^3 + 1$, $c = (1001110)$. In shift register implementations, bits come out of 0-degree term, recurrence is shifted into high-degree. Cyclic codes ideals in $\mathbb{Z}_2/(x^n - 1)$. Codewords are multiples of the generator polynomial $g(x)$. Let α be a primitive element of $GF(2^m)$. $[n = 2^m - 1, k = n - m, d = 3]$ hamming code has parity check $H = (1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2^m - 2})$. If $g(x)$ is the generator for α, generator matrix is

$$C = \begin{pmatrix} g(x) & 0 & 0 \\ 0 & xg(x) & 0 \\ 0 & 0 & x^2 g(x) \\ \ldots & & \end{pmatrix}$$

For BCH with $[n = 2^m - 1, k = n - 2m, d \geq 5]$, $g(x) = M^{(1)}(x)M^{(3)}(x)$ where $M^{(3)}(x)$, is the minimum polynomial for α^3.

BCH codes: If $g(x) | x^n - 1$, the ideal generated by $g(x)$ is a cyclic code. If $g(x)$ factors into linear factors in $GF(2^n)$ with roots $A = \{\alpha_1, \ldots, \alpha_r\}$, the set C defined by $f(x) \in C$ iff $f(\alpha) = 0, \forall \alpha \in A$ is a cyclic code. For BCH, pick $g(x) = m_1(x)m_2(x)\ldots m_r(x)$ of degree d with each factor irreducible. Let $n - d$ message bits be the high order coefficients $C_I(x)$ of an $n - 1$ degree polynomial whose remaining terms are $C_R(x)$ with $C_I(x) = g(x)q(x) + C_R(x)$. For a 2-ECC, pick $g(x) = m_1(x)m_2(x)$ with $m_1(x)$ the irreducible monic polynomial for a primitive nth root of 1, α and $m_2(x)$ the irreducible monic polynomial for α^3. Alternatively, suppose $g(x)$ is a cyclic code and α is a primitive nth root of $g(x)$ and $g(\alpha^l) = g(\alpha^{l+1}) = \ldots = g(\alpha^{l+\delta}) = 0$ then $d \geq \delta + 2$ and the resulting BCH code has weight d. Decoding BCH for $r = c + e$: (1) compute $(s_1, s_2) = rH^T$, (2) if $s_1 = 0$, no error, (3) if $s_1 \neq 0$ put $\frac{s_2}{s_1} = \alpha^{j-1}$, error is in position j (of $p \neq 2, e_j = \frac{s_1}{\alpha^{(j-1)(k+1)}}$), (3) $c = r - e$.

Reed-Solomon code is BCH code over F_q with $n = q - 1$. Let α be a primitive root of 1 and choose $d : 1 \leq d < n$ with $g(x) = (x - \alpha)(x - \alpha^2)\ldots(x - \alpha^{d-1})$. The BCH code generated by $g(x)$ is a Reed Solomon code (an MDS code too).

Building codes and Reed Muller: If $C_1 : (n, M_1, d_1)$ and $C_2 : (n, M_2, d_2)$, $C_3 = C_1 * C_2$ denotes the code where codewords in C_3 are $(u, u + v), u \in C_1, v \in C_2$. It is a $(2n, M_1 M_2, min(2d_1, d_2))$ code. $RM(0, m) = \{0, 1\}$, $RM(r+1, m+1) = RM(r+1, m) * R(r, m)$. $R(r, m)$ is a (n_r, M_r, d_r) code, with $n_r = 2^m$, $d_r = 2^{m-r}$ and $M_r = 2^a$, $a = 1 + \binom{m}{1} + \ldots + \binom{m}{r}$. $R(r, m)$ has parameters $[n = 2^m, k = 1 + \binom{m}{1} + \ldots + \binom{m}{r}, d = 2^{m-r}]$,

it consists of boolean functions whose polynomials are of degree $\leq m$. $RM(r,m)^{\perp} = RM(m-r-1,m)$.

$R = \frac{1-H_2(p)}{1-H_2(p_e)}$ (4,7) code. $U = \frac{H(K)}{D}$, 2^{RN} messages 2^{rN} meaningful ones, $2^{H(K)}$ keys. $2^{H(K)}-1$ keys have probability, q, of spurious decryption $R-r=D$. F= number of false ones. $F = (2^{H(K)}-1)q = 2^{(H(K)-D)N}$. The correct key maps cipher into meaningful class always. False keys map cipher into meaningful/meaningless randomly. After how many message is the expected number of spurious keys which map all the samples into meaningful less than 1? Shannon: M_C: total message length, M: meaningful part, p: probability of error. $pM_C = k$, $2^{M_C - M} \geq \binom{M_C}{k}$.

Hadamard Code: Let $h_{ij} = (-1)^{a_0 b_0 + \cdots + a_4 b_4}$, where a and b index the rows and columns respectively. This gives a 32×32 entry matrix, H. Let generators be $G = [H|-H]^T$. For each of the $0 \leq i < 2^6$ possible messages, send the row corresponding to i. To *decode Hadamard*, for the 32 bit received word, r, compute $d_i = r \cdot R_i$, where R_i is the 32 bit row i. If there are no errors, the correct row will have $d_i = 32$ and all other rows will have $d_i = 0$. If one error, $d_i = 30$, etc.

Definition: The *Golay Code* $\mathcal{G}_{24}$ is a $[24,12,8]$ linear code. $G = [I_{12}|C_0|N] = [I|B]$ where $C_0 = (1,1,1,1,1,1,1,1,1,1,1,0)^T$ and N is formed by circulating $(1,1,0,1,1,1,0,0,0,1,0)$ 11 times and appending an row of 11 1's. The first row of N corresponds to the quadratic residues (mod 11). Note that $wt(r_1+r_2) = wt(r_1) + wt(r_2) - 2[r_1 \cdot r_2]$, all codewords have weight divisible by 4 and $d(C) = 8$. $\mathcal{G}_{24} = \mathcal{G}_{24}^{\perp}$.

Decoding the Golay code: Let $G = [I_{12}|B]$ and $B^T = (b_1, b_2, \ldots, b_{12})$ with b_i a column vector. Suppose $r = c + e$ is received and $wt(e) \leq 3$. Put $s = rG^T$ and compute sB, $s + c_i^T$, $1 \leq i \leq 24$ and $sB + b_j^T$, $1 \leq j \leq 12$. If $wt(sB) \leq 3$, there is a non-zero entry in the k-th position of sB if the $k+12$-th position of e is non-zero. If $wt(s) \leq 3$ a non-zero entry in s at position k corresponds to a non-zero entry in position k of e. If $wt(s + c_j^T) \leq 2$, for some j, $13 \leq j \leq 24$ then $e_j = 1$ and non-zero entries of $s + e_j^T$ are in the same positions as non-zero entries of e. If $wt(sB + b_j^T) \leq 2$, for some j, $1 \leq j \leq 12$ then $e_j = 1$ and non-zero entries of $sB + b_j^T$ at position k correspond to non-zero entries of e_{k+12}.

Reed-Solomon construction: Fix n elements, $\langle \alpha_1, ..., \alpha_n \rangle$, $|F| \geq n$, $E(m) = \langle M\alpha_1, ..., M\alpha_n \rangle$, $d(E(m_1, m_2)) \leq n + k - 1$.

1.4.4 The Leech Lattice and the Conway groups

Background: Volume of n-sphere is $V_n r^n$ where $V_n = \frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}$. *Rogers Bound* is obtained by forming convex hull of $n+1$-simplex with spheres on vertices; volume interior to simplex and spheres forms upper bound. $RB(n) = \frac{\sqrt{(n+1)}(n!)^2 \pi^{\frac{n}{2}}}{2^{\frac{3n}{2}} \Gamma(\frac{n}{2}+1)} f_n(n)$, $F_{n+1}(\alpha) = \frac{2}{\pi} \int_{\frac{arcsec(n)}{2}}^{\alpha} F_{n-1}(\beta) d\theta$, $sec(2\beta) = sec(2\theta) - 2$, $F_1(\alpha) = F_0(\alpha) = 1$, $f_n(sec(2\alpha)) = F_n(\alpha)$. $RB(3) = .7404$. $A_1 = 0$, $A_{2n} = \begin{pmatrix} A_n & A_n \\ A_n & \overline{A_n} \end{pmatrix}$.

L_8: $v \in L_8$ iff $v \in \mathbb{Z}^8$ and $v_i = a_i \pmod 2$ or $v_i = \overline{a}_i \pmod 2$.

Generator matrix: $\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 \end{pmatrix}$.

$L_8 \to \Lambda_8$: $v \in \Gamma_8$ iff $v \in L_8$ and $\sum_{i=1}^{8} v_i = 4m$. Contact number: $112 + 128 = 240$, radius: $\sqrt{2}$. *Al-*

ternate definition of Λ_8: 8-tuples whose spheres are congruent $\pmod 2$ to rows of A_8 or $\overline{A_8}$. Density is $\frac{\pi^4}{4!2^4}$.

Definition: Let $R(C)$ be the row space of $\mathcal{G}_{24}$ over $GF(2)$. Define the *Leech Lattice*, Λ_{24}, as the vectors that satisfy the following conditions: Express coordinates in E_{24} in binary and retain the ones that satisfy the following conditions (a) the 24 1's bits are either all 0 or all 1, (b) the 2's bits form a row in $R(C)$, (c) 4's bits rows have even parity for points with 1's bits that are all 0 and odd otherwise. This is equivalent to the following: Suppose $\vec{c} \in R(C)$ and for $m \in \mathbb{Z}$, define $\vec{c}(m) = \{v \in \mathbb{Z}^{24} : \sum_i v_i = 4m, c_i = 0 \to v_i = m \pmod 4, c_i = 1 \to v_i = m + 2 \pmod 4\}$, $\Lambda = \Lambda_{24} = \cup_m \vec{c}(m)$.

Theorem: In Λ, lattice points are seperated by a minimum distance of $4\sqrt{2}$. Lattice points a minumum distance from the origin have shapes: $(0^{16}, (\pm 2)^8)$, $(0^{22}, (\pm 4)^2)$, $((\pm 1)^{23}, (\pm 3))$. Hence the contact number is 98256 (lattice point with even parity) + 98304 (lattice point with odd parity) = 196,560; the density is .001929. Each pair of adjacent lattice points is adjacent to 4600 others. *Example:* $(4, 4, 0, \ldots, 0)$ is adjacent to $(4, 0, \ldots, 0)$ - there are 88 of these, $(2, 2, \ldots, 0)$ - there are 77×2^7 of these and $(1, 3, \ldots, 0)$ - there are 2048 of these. For the first Leech packing, the density is $\frac{2^{24}}{2 \times 2^{12}} = 2^{-11}$, first factor of 2 in denominator is from condition that the sum of the coordinates $= 0 \pmod 4$ and so the packing density is .0009647. The Leech lattice doubles this which is about .8 of the Rogers bound.

Noting that there must be an even number of -2's, for the Leech packing, lattice points with even coordinates are:

Shape	**Number**
$0^{16}, (-2)^8$	759
$0^{16}, (-2)^6, 2^2$	$759 \cdot \binom{8}{2} = 21252$
$0^{16}, (-2)^4, 2^4$	$759 \cdot \binom{8}{4} = 53130$
$0^{16}, (-2)^2, 2^6$	$759 \cdot \binom{8}{2} = 21252$
$0^{16}, 2^8$	759
$0^{22}, (-2)^2$	$\binom{24}{2} = 276$
$0^{22}, -2, 2$	$24 \cdot 23 = 552$
$0^{22}, 2^2$	$\binom{24}{2} = 276$
Total	98256

The lattice points with odd coordinates are:

Shape	**Number**
$(-1)^{23}, 3$	24
$(-1)^{16}, (1)^7, -3$	$759 \cdot 8 = 6,072$
$(-1)^{15}, (1)^8, 3$	$759 \cdot 16 = 12,144$
$(-1)^{12}, (1)^{11}, -3$	$2576 \cdot 12 = 30,912$
$(-1)^{11}, (1)^{12}, 3$	$2576 \cdot 12 = 30,912$
$(-1)^8, (1)^{15}, -3$	$759 \cdot 16 = 12,144$
$(-1)^7, (1)^{16}, 3$	$759 \cdot 8 = 6,072$
$(1)^{23}, -3$	24
Total	98304

There are 4600 vertices adjacent to 2 adjacent simplex, 891 vertices adjacent to 3 adjacent simplex, 336 vertices adjacent to 4 adjacent simplex and 170 vertices adjacent to 5 adjacent simplex. This gives a dihedral like estimate on the size of the symmetry group.

Definition of Conway's group: .O is the set of rotations in $\mathbb{R}^{24}$ fixing O pointwise and Λ setwise.

Notation: $v_S = \sum_{i\in S} v_i$. $Q = \{x^2 : x \in F_{23}\}, N = \Omega \setminus Q$. $A + B = A \setminus B \cup B \setminus A$. $N_i = \{n - i, n \in N\}$. Golay code, $\mathcal{C}$, is generated by N_i, N_Ω. $N_A = \sum_{a\in A} N_a$. $C \in \mathcal{C}$ iff $N_C = 0$. $\Omega = PL(23)$, $\alpha : x \mapsto x + 1$, $\beta : x \mapsto 2x$, $\gamma : x \mapsto \frac{-1}{x}$, $\delta : x \mapsto 9x^3, x \notin Q$ and $\delta : x \mapsto \frac{x^3}{9}, x \in Q$. $L_2(23) = PSL_2(23) = \langle \alpha, \gamma\rangle$, $M_{24} = \langle \alpha, \gamma, \delta\rangle$. If $\pi \in S_\Omega$, define $(v_i)^\pi = v_{\pi(i)}$. $\epsilon_S(v_i) = -v_i, i \in S$ and $\epsilon_S(v_i) = v_i, i \notin S$.

Theorem: The set $G\Lambda = \{2v_K, K \in R(C)\} \cup \{v_\Omega - 4v_\infty\}$ generates Λ. If $v, w \in G\Lambda$, then $v \cdot v = 16n$ and $v \cdot w = 0 \,(\text{mod } 8)$. $\Lambda_n = \{x \in \Lambda, x \cdot x = 16n\}$. $\Lambda_1 = \emptyset$, Λ_2 consists of Λ_2^2 of shape $(0^{16}, (\pm 2)^8)$ - there are 97152 of these, Λ_2^3 of shape $((\pm 1)^{23}, (\pm 3)^1)$ - there are $98,304$ of these, Λ_2^4 of shape $(0^{22}, (\pm 4)^2)$ - there are 1104 of these. In tabular form:

Name	Shape	Number
Λ_2^2	$0^{16}, \pm 2^8$	$759 \cdot 2^7$
Λ_2^3	$\pm 1^{23}, \pm 3$	$24 \cdot 2^{12}$
Λ_2^4	$0^{22}, \pm 4^2$	$\binom{24}{2} \cdot 2^2$

Notation: If $S \in R(C)$, $\epsilon_S \in .O$. $E = \langle \epsilon_S\rangle_{S\in R(C)}$, $M = M_{24}$. $N = EM$. $T_0 = \{0, 3, 15, \infty\}$, $T_1 = \{1, 12, 21, 22\}$, $T_2 = \{2, 7, 11, 13\}$, $T_3 = \{4, 10, 16, 17\}$, $T_4 = \{5, 6, 9, 19\}$, $T_5 = \{8, 14, 18, 20\}$, $B = \{T_0, T_1, T_2, T_3, T_4, T_5\}$.

Theorem: $\lambda \in .O$ and λ fixes v_i (some i) iff $\lambda \in N$.

Proof of $\rightarrow$: Suppose $\lambda \in .O$ and $\lambda(v_i) = v_i$. If $\lambda(v_j) = w_j, i \neq j$ then $(v_i, w_j) = 0$. Since $4v_i + 4v_j \in \Lambda_2$, $4v_i + 4w_j \in \Lambda_2$. Examining the elements of Λ_2, we see $w_j = \pm v_k$ for some $k \in \Omega$ since $8w_j \in \Lambda$ and $4w_j \notin \Lambda$. Distinct values of j yield distinct values of k. Thus $\lambda = \pi\epsilon_S$, $S \subseteq \Omega, \pi \in S_{24}$. The non-zero coordinates of $\lambda(2v_K), K$ an octet are in the coordinate postions $\pi(K)$, so $\pi(K)$ is an octet and $\pi \in M_{24} = M$. $\lambda(v_\Omega - 4v_\infty)$ is a lattice point of the same shape and the coordinates are $= 1 \,(\text{mod } 4)$. $\epsilon_S : v_i \mapsto -v_i, i \in S$ so the coordinates of $\lambda(v_\Omega - 4v_\infty)$ which are $= 3 \,(\text{mod } 4)$ are in the places $\pi(S)$ and so $S \in R(C)$. So $\lambda = \pi\epsilon_S \in N$.

Theorem: If $\lambda(\Lambda_2^4) = \Lambda_2^4$ then $\lambda \in N$.

Proof: We use the following lemma:
Lemma: If $\lambda \in .O$ and $|\lambda| = p$, a prime then $p \leq 23$ further, no element of $.O$ has order $13 \cdot 23$.

Let H be the symmetries fixing Λ_2^4 as a whole and $x = 4v_i + 4v_j$ and N_x is the subgroup fixing x. N only changes signs and permutes coordinates so $N : \Lambda_2^4 \to \Lambda_2^4$ and fixes $\Lambda_2^4(x)$ as a whole. There are $2^2\binom{22}{2} = 924$ vectors of the form $\pm 4v_h \pm 4v_k$ are perpendicular to $\pm(4v_i - 4v_j)$ with h, i, j, k distinct and so are $\pm(4v_i - 4v_j)$. These 926 vectors form $\Lambda_2^4(x)$. N_x is 2-transitive so $\exists\sigma : (4v_i - 4v_j) \mapsto \pm(4v_i - 4v_j)$ and no other elements are in this orbit. Thus $\{(4v_i - 4v_j), -(4v_i - 4v_j)\}$ form a single orbit. $N_x \subseteq H_x$ and the orbits of H_x are a union of N_x orbits. As a result, it is either all 926 orbits or the N_x orbits. In the latter case, $|H_x : H_{x,y}| = 926 = 2 \cdot 463$ which contradicts the lemma. So we know H_x has 2 orbits on $\Lambda_2^4(x)$ and maps $(4v_i - 4v_j)$ to itself or it's negative. In the first case, $\lambda(v_i) = v_i$ and $\lambda \in N$ by the previous theorem. In the second case, $\lambda(v_i) = v_j$ and hence $(4v_i + 4v_h) \mapsto (\pm 4v_j \pm 4v_k), h \neq j$ and again $\lambda \in N$. Thus $H_x \subseteq N$ and $H_x \subseteq N_x$ and therefore $H \subseteq N$.

Theorem: There is a subgroup isomorphic to $L_2(23)$ which is transitive on octads.

Proof: There is a copy of $L_2(23)$ in M_{24}.

Definition: $\epsilon(v_i) = v_i$ if $i \notin Q$ and $-v_i$ if $i \in Q$.

Theorem: $N = \langle \alpha, \beta, \gamma, \delta, \epsilon \rangle$.

Proof: Applying permutations from the right, note $\epsilon_K = \epsilon\alpha\delta\alpha\epsilon\alpha^{-1}\delta^{-1}\alpha^{-1}$, $K = \{0, 1, 4, 5, 11, 12, 14, 22\}$. If L is another 8-set and $\theta : K \to L$ then $\epsilon_L = \theta^{-1}\epsilon_K\theta$.

Theorem: N is a proper subgroup of $.O$.

Proof: Let $T = T_0$ be any 4-set of Ω. T lies in 5, 8 sets $T + T_1, T + T_2, \ldots, T + T_5$, where T_i is the complement of T in the i-th 8-set. Ω is the disjoint union of 6, 4-sets. $B = \{T_0, T_1, \ldots, T_5\}$. $\eta = \eta_B : v_i \mapsto v_i - \frac{1}{2}v_{T_j}$ and $\zeta_T = \eta\epsilon_T$. $\zeta_T^2 = 1$. $\zeta_T \in .O$ and $\zeta_T \notin N$.

Theorem: H_x is transitive on $\Lambda_2(x)$.

Proof: Let $x = v_\Omega - v_\infty$. The order of each orbit of H_x on $\Lambda_2(x)$ has order divisible by 23.

Theorem: If $H > N$, H is transitive on Λ_2 and $H = .O$. $|.O| = 2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23 = 8,315,553,613,086,720,000$.

Proof: (1) Λ_2^2, Λ_2^3, Λ_2^4 are all N-orbits. A counting argument shows that the union of two of them can't be an H orbit (otherwise, $p \mid |.O|$ for $p > 23$). Now define $\Lambda_2(x) = \{y : y \in \Lambda_2, y \perp x\}$. Recall H_x is transitive on $\Lambda_2(x)$. Since M_{24} is $5-$transitive $|H_x : H_{x,y}| = 926$ and $|.O| = |H| = 196560 \cdot |H_x|$; further, H_x is transitive on $\Lambda_2(x) = \{y : y \perp x\}$. An orbit of H_x has 93150 elements so $|H_x| = (93150)|H_{x,y}|$ and $H_{x,y} = E_{10}M_{22}$. This gives the order of H and shows $H = .O$.

Definition: For $x \in \Lambda_2$, define $\{x, -x\}$ is called a diameter. $\overline{\Lambda_2}$ is the set of 98280 diameters. $.1 = .O_d, d = \{x, -x\}, x \in \Lambda_2$

Theorem: N is maximal in $.O$. $.O = \langle N, \zeta \rangle$.

Proof: By the theorem, if $H > N$, $H = .O$. The second statement follows from $\zeta \notin N$ and $\zeta \in .O$.

Theorem: $.O$ is transitive on ordered pairs of points of vectors of Λ_2 with a given scalar product.

Proof: $\Lambda_2 = \{v \in \Lambda : v \cdot v = 16 \cdot 2\}$. By looking at products of vectors of standard type, the possible products are $0, \pm 8, \pm 16, \pm 32$. Put $\Lambda_2(x, m) = \{y : (x, y) = m\}$. We find orbits of N_x on $\Lambda_2(x, 16)$ and show $\Lambda_2(x, 16)$ is a single orbit of $.O_x$.

Observation: Let φ be an octad, say $\{0, 1, 2, 3, 4, 7, 10, 12\}$, and $i \notin \varphi$; suppose K is the subgroup fixing φ, setwise and $H = K_i$. The subset fixed is of codimension 8 so it has dimension 4. K acts naturally on this 4-dimensional subspace. $K \approx 2^4 L_4(2)$.

Theorem: $.1 \cong .O/\mathbb{Z}(.O)$ and $|\mathbb{Z}(.O)| = 2$.

Proof: Suppose $\lambda \notin \{\pm 1\} \in \mathbb{Z}(.O)$. $\theta_i = \alpha^{23-i}\gamma\alpha\gamma\alpha^i$ fixes i and moves all other points of Ω. (1) λ cannot send $v_j \mapsto \pm v_j, \forall j$ since $(v_j)\lambda\alpha = -v_{j+1}$ and $(v_j)\alpha\lambda = v_{j+1}$. (2) λ cannot map $v_i \mapsto \pm v_j, i \neq j$, $(v_i)\lambda\theta_i = \pm(v_j)\theta_i = \pm v_k \neq \pm v_j$, but $(v_i)\theta_i\lambda = \pm(v_j)$. (3) Remaining case, namely, $\lambda : v_i \mapsto w \neq \pm v_j, j \in \Omega$ is impossible too. If $(v_j)\lambda = w \neq \pm v_k$, any k. $(8v_i)\lambda \in \Lambda_4$ and has one of the following form $(0^{23}, \pm 8^1)$, $(\pm 0^{20}, \pm 4^4)$, $(\pm 0^{16}, \pm 2^7, \pm 6^1)$, $(\pm 0^{14}, \pm 2^8, \pm 4^2)$, $(\pm 0^{11}, \pm 2^{12}, \pm 4^1)$, $(\pm 0^8, \pm 2^{16})$, $(\pm 1^{21}, \pm 3^2, \pm 5^1)$, $(\pm 1^{19}, \pm 3^5)$. The only one fixed by θ_i is $8v_i$. Thus $(v_i)\lambda\theta_i = (w)\theta_i \neq w$ but $(v_i)\theta_i\lambda = w$ and the theorem holds.

Theorem: .1 acts primitively on $\overline{\Lambda_2}$.

Proof: Each element of .1 permutes 98280 diameters. Since $.O$ is transitive on Λ_2, .1 is transitive for diameters. Suppose .1 is imprimitive. $|S_1| \mid 98280$. Let $\overline{x} \in S_1$. Since $|S_1| \geq 1, \exists y \in S_1$ whose orbit under $.1_{\overline{x}}$ has order $4600, 47104, 46575$. Since .1 fixes $\overline{x}$, $.1 : S_1 \to S_1$ and $|S_1| \geq 4601$. None divide 98280 so $\exists \overline{z} \neq \overline{x}$ outside S_1. But then S_1 which has at least $1 + 4600 + 46575 = 51176$ and thus must be all of $\overline{\Lambda_2}$. This contradicts the assumed imprimitivity of .1.

Theorem: $.1 = .O/\mathbb{Z}(.O)$ is simple.

Proof: Suppose $\mathbb{Z}(H) \subsetneq H \subsetneq .O$. (1) H is transitive on $\overline{\Lambda_2}$. If not $\exists \overline{x} = \{x, -x\}$ and $y \in \Lambda_2 : \eta(x) = y, \eta \in H$. $.O$ is transitive on $\overline{\Lambda}_2$. Orbits of H in $\overline{\Lambda}_2$ are of equal size. (2) N is not normal in .0. This is proved by looking at B, the 4-subsets defined above. (3) $H = N$. $|H : H_x| = 13 \cdot 7560$. Let $P \in S_{13}$. Since H is normal, all the sylow 13 subgroups of $.O$ are in H so $| > O : N_{.O}(P) = |ccl_{.O}(P)| = |ccl_H(P)| = |H : N_H(P)|$ and $|.O : H| = |N_{.O}(P) : N_H(P)|$ with $N_H(P) = N_{,O}(P) \cap H$. Thus $|.O| = |N_{.O}(P)H| = \frac{|N_{.O}(P)| \cdot |H|}{|N_{.O}(P) \cap H|}$ and $23 \mid |N_{.O}(P)|$ or $23 \mid |H|$. In the former case, put $K = \langle \lambda \rangle$, $P = \langle \mu \rangle$, $|\lambda| = 13$, but then $|PK| = 13 \cdot 23$ which contradicts an earlier lemma. In the latter case, $23 \mid |H|$ so $H \cap N = N$ but N is maximal so $H = N$. Now we have $H \lhd .O$ and $H = N$ but N is not normal and this establishes the result. $\zeta \in .1 : x \mapsto z$, $\lambda \in H : x \mapsto w$. $\zeta(w) = \zeta(\lambda(x)) = \zeta\lambda\zeta^{-1}(z)$ is in orbit of z since $\zeta\lambda\zeta^{-1} \in H$. .1 preserves orbits in Λ_2 and the orbits are sets of imprimitivity for .1 on $\overline{\Lambda}_2$ which contradicts the previous result. For $x \in \overline{\Lambda}_2$, $|H : H_x| = |\overline{\Lambda}_2| = 98280 = 13 \cdot 7560$. Let $P \in S_{13}(H)$ all such are H conjugate and $|.O : N_{.O}(P)| = |H : N_H(P)|$.

Conway's other simple groups: $.2 = \{x \in .O,\ x$ stabilizes 2 points $v, w \in \Lambda_2 : |v - w| = 4\sqrt{2}\}$. $.3 = \{x \in .O$, where x stabilizes 2 points $v, w \in \Lambda_2 : |v - w| = 4\sqrt{3}\}$.

1.5 Algebraic Geometry

1.5.1 Basics

Theorem: Every conic in the affine space over R is equivalent under an affine transformation to one of the following: (1) $X^2 + Y^2 + P = 0$ (ellipse, point, empty set), (2) $X^2 - Y^2 + P = 0$ (hyperbola, intersecting lines), (3) $X^2 + Y + P = 0$ (parabola), (4) $X^2 + P = 0$ (parallel lines, point empty). In projective space (1), (2), (3) are equivalent. In the projective space over $\mathbb{C}$, they are all projectively equivalent.

Definitions: Let $R = k[x_1, \ldots, x_n]$, $W = k^n = \mathbb{A}^n$ for the *affine* setup and $R = k[x_0, x_1, \ldots, x_n]$ (where $f \in R$ is a *homogeneous* polynomial), $W = k^{n+1} \setminus \{\vec{0}\} = \mathbb{P}^n$ under the usual equivalence for the *projective* setup. If $S \subseteq R$, $V(S) = \{x \in W : f(x) = 0, \forall f \in S\}$. $V(S)$ is an *affine* (resp *projective*) *algebraic set.* An algebraic set is *irreducible* if is cannot be expressed as the union of two non-trivial algebraic sets. An affine irreducible algebraic set is an *algebraic variety.* If $S = \{f\}$, $V(S)$ is called a *hypersurface.* If $V \subseteq W$, $I(V) = \{f \in R : f(x) = 0, \forall x \in V\}$. If $\langle S \rangle = I$ as an ideal in R, $V(S) = V(I)$. $rad(I) = \sqrt{I} = \{a : a^n \in I\}$. I is a *radical* ideal if $I = \sqrt{I}$. Roughly, radical ideals $\leftrightarrow$ varieties, prime ideals $\leftrightarrow$ subvarieties, maximal ideals $\leftrightarrow$ points. If V is an algebraic variety, $I(V)$ is a prime ideal (proof below) and $\Gamma[V] = R/I(V)$ is called a *coordinate ring.* $\overline{R} = k(x_1, \ldots, x_n)$ is the quotient field of R; members of $\overline{R}$ induce *rational* maps. $\mathcal{O}_P(V)$ denotes the rational functions on V defined on P. The *Zariski* topology on W is defined by identifying the $V(S)$ with *closed sets.*

Theorem: Let k be algebraically closed. There is a one to one correspondence between polynomial maps $\varphi : V \to W$ and the homomorphisms $\tilde{\varphi} : \Gamma[W] \to \Gamma[V]$. Let $\mathcal{T}(V, k) = \{f : f : V \to W\}$. If $\varphi : V \to W$, $\tilde{\varphi} : \mathcal{T}(W, k) \to \mathcal{T}(V, k)$.

Theorem: $k \subseteq \Gamma[V)] \subseteq \mathcal{O}_P(V) \subseteq k(V)$.

Definitions: Two affine varieties V, W are *isomorphic* if $\exists \phi, \psi : \phi \circ \psi = id_W$. Suppose F_i is a collection of functions. The *multiplicity of a root* at a point $\vec{a}$ is $f(t) = gcd(F_1(\vec{a} + L(t)), \ldots, F_m(\vec{a} + L(t)))$ where $L(t)$ is a line through $O = \vec{0}$. By transferring P to $\vec{0}$ and express $F = F_m + \ldots + F_n$, F_m is a form of degree m. L touches X at O if its intersection multiplicity is greater than 1. Locus of points touching X at x is the *tangent space*, $\Theta_{x,X}$. Two varieties V, W are *birationally equivalent* if there are *rational* maps $\varphi_1 : V \to W$ and $\varphi_2 : W \to V$ between them. $f(x, y)$ is *rational* if $\exists \phi, \psi$: $f(\phi(t), \psi(t)) = 0$. Any conic (2nd order equation) in two variables has either infinitely many rational solutions or none.

Theorem: Two curves are birationally equivalent iff their fields of functions are isomorphic.

Theorem: Every irreducible curve of degree 2 is rational. $x^n + y^n = 1$ is not rational for $n > 2$.

Definition: Suppose $\phi : A^n(k) \to A^m(k)$, $f \in k[y_1, \ldots, y_m]$; the *pullback* is $\phi^* : \phi^* \circ f = f \circ \phi$. A *discrete valuation ring ("DVR")* is a Noetherian, local domain whose maximal ideal is principal. If a form, F, does not vanish on an irreducible projective variety X then $dim(X_F) = dim(X) - 1$.

Theorem: The following are equivalent: (1) The set of non-units in R form an ideal; (2) R has a unique

maximal ideal. The following are equivalent and define a DVR: (1) R is Noetherian and its maximal ideal is principal; (2) $\exists t \in R : \forall 0 \neq z \in R : z = ut^n$, where u is a unit.

Proof: We show $1 \to 2$. First uniqueness. If $ut^m = vt^n$ for units u, v, $ut^{m-n} = v$ but then t^{m-n} is a unit. For existance, since $\mathfrak{m} = (t)$, for a non-unit, $z \in \mathfrak{m}$, $z = z_1 t$ and if z_i is a non-unit, $z_{i+1} = z_i t$ so $(z_1) \subset (z_2) \subset \ldots$ and since R is Noetherian eventually $(z_n) = (z_{n+1})$. $z_{n+1} = vz_n, v \in R$ $z_n = tvz_n$ so $vt = 1$ but t is not a unit.

Theorem: The pole set is an algebraic variety. $\Gamma[V] = \bigcap_{P \in V} \mathcal{O}_P(V)$.

Theorem: If $S_1 \subseteq S_2$ then $I(S_1) \supseteq I(S_2)$. Every algebraic set is the intersection of hypersurfaces.

Proof: By the Hilbert basis theorem, $I(V) = (f_1, f_2, \ldots, f_r)$ and so $V = V(f_1) \cup \ldots \cup V(f_r)$.

Theorem: Every closed set is the union of finitely many irreducible ones. Every irreducible closed set is birationally isomorphic to a hypersurface in A^n.

Theorem: (1) An algebraic set, V, is irreducible iff $I(V)$ is prime. (2) If k is algebraically closed, $I(V(f)) = (f)$. (3) If I is radical, $I(V(I)) = I$.

Proof: (3) follows from Nullstellensatz.

Theorem: Let $R = k[x, y]$. If $f, g \in R$ have no common factor, $V(f) \cap V(g)$ is finite.

Proof: $k(x)[y]$ is a PID, $Af + Bg = 1$ over $k(x)$; now clear denominators.

Theorem: If I is prime, $V(I)$ is irreducible. There is a $1-1$ correspondence between prime ideals and irreducible algebraic sets; there is a $1-1$ correspondence between maximal ideals and points.

Theorem: Let V be an algebraic set then $V = V_1 \cup \ldots V_r$, V_i, irreducible, $V_i \nsubseteq V_j, i \neq j$.

Proof: We use the following (follows from axiom of choice). Let $\mathcal{S}$ be a non-empty collection of ideals in a Noetherian ring, R, then $\mathcal{S}$ has a maximal element. From this we conclude and collection of algebraic sets has a minimal element.
Now let $\mathcal{S} = \{V : \text{algebraic, } V \text{ is not a finite union of irreducible algebraic sets}\}$. Let V be a minimal element of $\mathcal{S}$. $V = V_1 \cup V_2$ and this is a contradiction. For the second condition, throw out the V_i violating it.

Theorem: $\mathcal{O}_P(V)$ is a Noetherian local domain. Further, the maximal ideal $\mathfrak{M}_P(V)$ is generated elements of $f \in \Gamma[V]$ for which $f(P) = 0$.

Proof: STS $I \subseteq \mathcal{O}(V)$ is finitely generated. Since $\Gamma[V]$ is Noetherian, $(f_1, \ldots, f_r) = I \cap \Gamma[V]$. Claim $(f_1, \ldots, f_r) = I$ and an $\mathcal{O}(V)$ ideal, for if $f \in I$, $\exists b \in \Gamma[V] : b \neq 0$ and $bf \in \Gamma[V]$ so $bf = \Gamma[V] \cap I$, $bf = \sum_i a_i f_i, a_i \in \Gamma[V]$ and $f = \sum_i \frac{a_i}{b_i} f_i$.

Definition: $I(P, F \cap G) = dim_k(\mathcal{O}_P(\mathbb{A}^2)/(F, G)$.

Theorem: $|V(I)| < \infty$ iff R/I is finite dimensional over k.

Proof: If $P_1, \ldots, P_r \in V$, we can fine $f_i \in R : f_i(p_j) = \delta_{ij}$ so $r \leq dim_k(R/I)$. On the other hand, if $V(I) = \{P_1, P_2, \ldots, P_r\}, P_i = (a_{i1}, a_{i2}, \ldots, a_{in})$, define $f_j = \prod_i (x_i - a_{ij}), F_j \in I(V(I))$ so $F_j^N \in I, \overline{F}_j = 0$ and $\overline{X}_j^{rN}$ is a k-linear combination of $\overline{1}, \overline{x}_j^1, \ldots, \overline{x}_j^{rN-1}$ and $\overline{x}_1^{m_1}, \ldots, \overline{x}_n^{m_n}; m_i < rN$ is a set of generators.

Theorem: Let I be an ideal of R (k, algebraically closed), $V(I) = \{P_1, \ldots, P_N\}$ and $\mathcal{O}_i = \mathcal{O}_{P_i}(\mathbb{A}^n)$, $\exists \varphi : R/I \to \prod_i \mathcal{O}_i/(I\mathcal{O}_i)$ induced from the natural homomorphisms $\varphi_i : R \to \mathcal{O}_i/(I\mathcal{O}_i)$.

Theorem: P is a simple point of f iff $\mathcal{O}_P(V(f))$ is a DVR. If L is a non-tangent line $l + \mathcal{O}_P(V)$ is a uniformizing parameter.

Proof: WLOG, $P = (0,0), L = ax$ and $y = 0$ is the tangent. $\mathfrak{M}_P(V(f)) = (x, y)$ whether P is simple or not. Suppose $f = y(1 + g(x,y)) - x^2 h(x)$ and $yg = x^2 h \in \Gamma(f)$ so $y = x^2 h g^{-1}$ since $g(P) \neq 0$ and $\mathfrak{M}_P(V(f)) = (x)$.

Theorem: Suppose $\mathfrak{M} = \mathfrak{M}_P(F)$ denotes the maximal ideal of $\mathcal{O} = \mathcal{O}_P(F)$. $0 \to \mathfrak{M}^n/\mathfrak{M}^{n+1} \to \mathcal{O}/\mathfrak{M}^{n+1} \to \mathcal{O}/\mathfrak{M}^n \to 0$. $\chi(n) = dim(\mathcal{O}/\mathfrak{M}^n) =$ Hilbert polynomial.

Theorem: Let P be a point on an irreducible curve, f, for all sufficiently large n, $m_P(f) = dim_k(\mathfrak{M}_P(f)^n/\mathfrak{M}_P(f)^{n+1})$.

Divisors: Suppose $E : y^2 = x^3 - x$ and $f(x,y) = \frac{x}{y}$. On $E : \frac{x}{y} = \frac{y}{x^2-1}$. If u_P is a *uniformizer*, $f = u_P^r g, r \in \mathbb{Z}, g(P) \neq 0, \infty$ and we define $ord_P(f) = r$. In this example, $u_{(0,0)} = y$ is a uniformizer at $(0,0)$ of $E : y^2 = x^3 - x$. Since $x = y^2(\frac{1}{x^2-1}) = y\frac{y}{x^2-1} = \frac{x}{y}y = x$, $ord_{(0,0)}(x) = 2$. In general, for $P = (x_0, y_0) \in E$, u_P can be taken as any line through P not tangent to E, thus we can take $u_P = x - x_0$ when $y_0 \neq 0$ and $u_p = y$ when $y_0 = 0$. For example, if $E : y^2 = x^3 + 72$ then $(-2, 8) \in E$. Since $f(x,y) = x + y - 6$ vanishes at $(-2,8)$ and $f(x,y) = (x+2) + (y-6) = (x+2)(1 + \frac{(x+2)^2 - 6(x+2)+12)}{y-8})$, $ord_P(f) = 1$, $u_\infty = \frac{x}{y}$.

Weak Bezout: If two curves of dimension m and n meet at more than mn points (counting multiplicity) then they have a common component.

Proof: Strategy of Proof: (S-1) $\#(C_1 \cap C_2 \cap \mathcal{A}^2) \leq dim(\frac{R}{(f_1,f_2)}) \leq n_1 n_2$, (S-2) first inequality is an equality, (S-3) first inequality can be strengthened to $I(C_1 \cap C_2, P) \leq dim(\frac{R}{(f_1,f_2)})$, (S-4) inequality in 4 is an equality, (S-5) I is invariant under projective transformations — transform so the line at infinity does not intersect $C_1 \cap C_2$. Notation: Let $f_1(x,y)$, and $f_2(x,y)$, defining curves C_1 and C_2, have dimension m, n respectively. $R = k[x,y]$, $(f_1(x,y), f_2(x,y)) = Rf_1 + Rf_2$.

S-1: $C_1 \cap C_2 \leq dim_k(\frac{R}{(f_1,f_2)}) \leq mn$. [Argument: If $P_1, P_2, \ldots P_r$ are distinct, $\exists h_i(x,y)$ with $h_i(P_j) = \delta_{ij}$, so if there are r common roots of f_1 and f_2, $\sum_{i=1}^r c_i h_i(x,y) = r_1 f_1(x,y) + r_2 f_2(x,y)$ implies $c_i = 0$.]
Let R_d be polynomials of degree $\leq d$ then $dim_k(R_d) = \phi(d) = \frac{(d+1)(d+2)}{2}$. Let $W_d = R_{d-m} f_1 + R_{d-n} f_2$, for $d \geq (m+n)$. $R_{d-m} f_1 \cap R_{d-n} f_2 = R_{d-m-n} f_1 f_2$. $dim_k(R_d) - dim_k(W_d) = mn$. $g = \sum_i^l c_j g_j$ has a non-trivial dependency for $l > mn$ with $g \in W_d$.
S-2: Second inequality is equality if $C_1 \cap C_2$ don't meet at infinity. Let f^* be the homogeneous polynomial consisting of the highest degree terms in f. If $\infty \notin C_1 \cap C_2$ then f_1^*, f_2^* have no common factor. If f_1^* and f_2^* have no common factor then $(f_1, f_2) \cap R_d = W_d$. Under the conclusion of the previous sentence, if $d \geq n_1 + n_2$ then $dim(\frac{R}{(f_1,f_2)}) \geq n_1 n_2$ which proves the result.

Define $\mathcal{O}_P = \{F \in K(x,y) : F(P) \text{ exists }\}$, $\mathfrak{M}_P = \{f \in \mathcal{O}_P : f(P) = 0\}$. $\mathfrak{M}_P$ is a unique maximal ideal of O_P. $(f_1, f_2)_P = f_1 O_P + f_2 O_P$. Now define $I(C_1 \cap C_2; P) = dim(\frac{\mathcal{O}_P}{(f_1,f_2)_P})$.
S-3: $\frac{\mathcal{O}_P}{(f_1,f_2)_P} \leq \frac{R}{(f_1,f_2)} < \infty$. $\mathcal{O}_P = (f_1, f_2)_P + R$. If $P \notin C_1 \cap C_2$ then $I(C_1 \cap C_2, P) = 0$; If $P \in C_1 \cap C_2$ then $(f_1, f_2)_P \subset \mathfrak{M}_P$; $I(C_1 \cap C_2; P) = 1 + dim(\frac{R}{(f_1,f_2)_P})$ iff $(f_1, f_2) = \mathfrak{M}_P$. If $P \in C_1 \cap C_2$ and $r \geq dim(\frac{\mathcal{O}_P}{(f_1,f_2)_P})$ then $\mathfrak{M}_P^r \subset (f_1, f_2)_P$. If $P, Q \in C_1 \cap C_2 \cap \mathcal{A}^2, \psi \in \mathcal{O}_P$ then $\exists g \in R$: $g = \psi \,(\text{mod } (f_1, f_2)_P)$ and $g = 0 \,(\text{mod } (f_1, f_2)_Q)$ if $P \neq Q$.
S-4: Kernel of natural map $R \to \prod_{P \in (C_1 \cap C_2 \cap \mathcal{A}^2)} \frac{\mathcal{O}_P}{(f_1,f_2)_P}$ is just (f_1, f_2) where the natural map is: $f \mapsto (\ldots, f \,(\text{mod } (f_1, f_2)), \ldots)$. $dim(\frac{R}{J}) = \sum_P dim(\frac{\mathcal{O}_P}{(f_1,f_2)}) = \sum_P I(C_1 \cap C_2, P)$. The last equality holds iff $J \subset (f_1, f_2)$. Define $L = \{g \in R : gf \in (f_1, f_2)\}$ and $1 \in L$. L is an ideal $(f_1, f_2) \subset L \subset R$. $P \in \mathcal{A}^2$, $\exists g \in L : g(P) = 0, P \in L$. $\exists a \in k : 1 \notin L + R(x - a)$ and $\exists b \in k : 1 \notin L + R(x - a) + R(y - b)$.
S-5: Properties of intersection multiplicity. $I((y - x^m), y; 0) = m$. Show the definitions make sense and that there is a line L which does not contain any of the intersection points. The proof requires knowing there are only a finite number of points in the intersection.

Genus for non-singular curve: $g_f = \frac{(n-1)(n-2)}{2} - d$. $L(D) = \{f : K(C)^* : div(f) \geq -D\}$. $l(D) = dim(L(D))$.

Reimann Roch Theorem: Let X be a non-singular projective plane curve. $\exists g \geq 0 : \forall D, dim_k(L(D)) \geq deg(D) + 1 - g$. The minimum such g is called the genus.

Resultants: The r forms $f_1, f_2, ..., f_r$ with indeterminate coefficients possess a resultant system of integral polynomials b_k such that for special values of the coefficients in K (algebraically closed). The vanishing of all resultants is a necessary and sufficient condition for $f_1 = f_2 = ... = f_r = 0$ to have a solution $\neq 0$. The b_k are homogeneous in the coefficients of every form f_i and satisfy $x_k^{s_r} b_k = 0 \,(\text{mod } (f_1, f_2, ..., f_r))$.

Bezout's Theorem. If f, g are two curves of degree n, m respectively that have no common component then they intersect in mn points counting multiplicity. Notes: A homogeneous system $f_1 = f_2 = ... = f_r = 0$ has solutions $(\xi_1^{(a)}, \xi_2^{(a)}, ...\xi_n^{(a)}), a = 1, 2, 3, ..., q$. Set $l_x = u_1 x_1 + u_2 x_2 + ... + u_n x_n$. Form resultant system $b_1(u), ..., b_t(u)$. The common zeros of $b_1, ...$ are $\prod l_a$. By Nullstellensatz, $(\prod_a l_a)^\tau = 0(b_1(u), b_2(u), ..., b_t(u))$ $\to D(u) = \prod {l_a}^{\rho_a}$ and $(b_i(u))^{r_i} = 0(\prod l_a) \to D(u) = (f_1, ..., f_r, l)$. $R(u)$ is the same as the u-resultant so $\sum \rho_a$ is the degree of $R(u) = \prod deg(f_i)$.

Example: $F_1(x, y, z) = x^2 + y^2 - 10z^2 = 0$, $F_2(x, y, z) = x^2 + xy + 2y^2 - 16z^2 = 0$, add $F_3(x, y, z) = u_0 z + u_1 x + u_2 y$. $Res_{1,2,2}(F_0, F_1, F_2) = (u_0 + u_1 - 3u_2)(u_0 + 2\sqrt{2}u_1 + \sqrt{2}u_2)(u_0 - 2\sqrt{2}u_1 - \sqrt{2}u_2)$. Solutions are $(1, -3, 1)$, $(-1, 3, 1)$, $(2\sqrt{2}, 2\sqrt{2}, 1)$, $(-2\sqrt{2}, -2\sqrt{2}, 1)$.

Example proof with generics: $F_1(X, Y, Z) = X - Y^2$, $F_2(X, Y, Z) = XY - Z$, $(X, Y, Z) \to (t^2, t, t^3)$ is generic because it is a solution for any specialization of t and any solution is obtainable this way.

Let D be a domain and $\Omega = \Omega_D = \overline{D(t_1, t_2, ...)}$ is called a universal field. Note that $\Omega \leftrightarrow$ prime ideals over $D[X_1, ...]$.

Theorem: $x_1, ...x_n \in \Omega$. $I = \{f : f(x_1, ..., x_n) = 0\}$ is a prime ideal. If I is a prime ideal and $1 \notin I$ then I has a generic 0. Any extension $K(\alpha_1, ..., \alpha_m)$ can be embedded in Ω.
Hints: look at $E = D[X]/I$. Under this homomorphism the image of $(X_1, ...X_n)$ is generic.

Theorem: If $\xi_1, ..., \xi_n$ are elements of an arbitrary extension of K then If $\Re = K[X_1, ..., X_n]$ and $\wp = \{f : f(\xi_1, ..., \xi_n) = 0\}$. $1 \notin \Re$ and $\wp$ is a prime ideal. Every prime ideal has a generic element.

Theorem: Any ideal $g = (f_1, ..., f_n)$ which has no zeros in Ω is the unit ideal. *Proof:* Otherwise a maximal ideal would correspond to a non-zero generic point.

Extension of Nullstellensatz: If $p_1, ..., p_s$ all vanish at the common zeros of $(f_1, ..., f_n)$, then $\exists q$ such that powers of the p_i's of degree q are in $(f_1, ..., f_n)$.

> *Proof:* For $s = 1$, this is the simple Nullstellensatz. Let the exponent for each i be q_i. Set $q = q_1 + q_2 + ... + q_n - n + 1$. Nullstellensatz bound: $\rho \leq 13d^n$ where d is the degree and n is the number of variables.

Theorem: Let N_q be the number of products X_j of degree q. Suppose $F_1, F_2, ..., F_r$ are forms. $(0, ..., 0)$ is the only common zero iff all products X_j can be expressed as linear combinations of the $X_{ki}F_i$ with coefficients in K. Note: This means they are linearly independent. So there are other common zeros is there are fewer than N_q. Note that $X_1, ..., X_n$ satisfy the extension conditions. If the $X_{ki}F_i = \sum a_{kij}X_j$ are not linearly independent, the determinant families, $R_i(a)$, form a resultant set.

Multivariate resultants: If we fix degrees $d_0, d_1, \ldots d_n$ then there is a unique polynomial $Res \in \mathbb{Z}[u_i, \alpha]$ such that (a) if $F_0, F_1, \ldots, F_n$ are homogeneous polynomials of degrees $d_0, d_1, \ldots d_n$ then $F_0 = \ldots = F_n = 0$ has a nontrivial solution over $\mathbb{C}$ iff $Res(F_0, \ldots, F_n) = 0$, (b) $Res(x_0^{d_0}, \ldots, x_n^{d_n}) = 1$, (b) , (c) Res is irreducible in $\mathbb{C}[u_i, \alpha]$. If $PP = PP(x_1, x_2, \ldots, x_n)$ is a set of power products in the x_i, there are $N_m = \binom{m+n-1}{n-1}$ PP's of degree m. *Example:* $A_3 = a_3x^2b_3y^2 + c_3z^2$, $A_2 = a_2x + b_2y + c_2z$, $A_1 = a_1x + b_1y + c_1z$. $S_i = \frac{PP_i^d}{x_i^d}$, $S_1 = \langle x^2, xy, xz\rangle, S_2 = \langle y^2, yz\rangle, S_3 = \langle z^2\rangle$.

	x^2	xy	xz	y^2	yz	z^2
xA_1	a_1	b_1	c_1	0	0	0
yA_1	0	a_1	0	b_1	c_1	0
zA_1	0	0	a_1	0	b_1	c_1
yA_2	0	a_2	0	b_2	0	0
zA_2	0	0	a_2	0	b_2	c_2
A_3	a_3	0	0	b_3	0	c_3

1.5.2 Elliptic Curves

Basic Definitions: An *elliptic curve* is a smooth projective curve of genus 1 with a distinguished point O. In the plane, (affine) elliptic curves are described by an equation of the form $E(F) : y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in F$ called the *general affine Weierstrauss form (GWF).* An equation of the form $E(F) : y^2 = x^3 + ax + b$, $a, b \in F$, is said to be in *special affine Weierstrauss form (SWF)* and sometimes we denote this curve by $E_{a,b}(F)$. If $P = (x_P, y_P)$ is a solution of the SWF, P is said to be on the elliptic curve $E_{a,b}(F)$.

Definitions: *Projective coordinates:* $(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$, $X_1 = \lambda^c X_2$, $Y_1 = \lambda^d Y_2$, $Z_1 = \lambda Z_2$, $c, d \in \mathbb{Z}^{>0}$ and usually $c = d = 1$. *Jacobian projective coordinates:* $\infty = (1 : 1 : 0)$ and $-(X : Y : Z) = (X :$

$-Y : Z)$. *Standard projective coordinates:* $\infty = (0 : 1 : 0)$ and $-(X : Y : Z) = (X : -Y : Z)$.

Addition Formula for SWF: $Y^2Z = X^3 + aXZ + bZ^3$, $P_i = (x_i, y_i)$, $O = (0 : 1 : 0)$. We want to calculate $R = P_1 + P_2$. If P_1 or P_2 is O, result is obvious. If $x_1 = x_2$ and $y_1 = -y_2$, $R = O$. If $x_1 \neq x_2$, set $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$. If $x_1 = x_2$ and $y_1 \neq -y_2$, set $\lambda = (3{x_1}^2 + a)(y_1 + y_2)^{-1}$. In either case, $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ and $R = (x_3 : y_3 : 1)$. $|\epsilon_p| \leq 2\sqrt{p}$. $E_{a,b}(F)$ defined by $f(x, y) = y^2 - (x^3 + ax + b)$ is *non-singular* if there is no point $(x, y) \in E_{a,b}(F)$ such that $\frac{\partial f}{\partial x}(x, y) = 0$ and $\frac{\partial f}{\partial y}(x, y) = 0$ or equivalently provided $x_a^3 x + b$ does not multiple roots. $f(x, y)$ has multiple roots iff $-(4a^3 + 27b^2) = 0$. Usually we pick Z axis tangent to O and then $(0, 1, 0)$ as the point at ∞.

Theorem: If C_1 and C_2 are two non cubic curves that meet at eight points, they meet at nine points (counting multiplicity).

Proof: $C_1 : a_1x^x + a_2y^3 + \ldots + a_{10}xyz$. $C_2 : b_1x^x + b_2y^3 + \ldots + b_{10}xyz$. The set of cubics passing through eight points form a two parameter family: $C = \alpha C_1 + \beta C_2$. $C_1(P_i) = 0 = C_2(P_i), i \leq 8 \rightarrow C(P_9) = 0$.

Observation: The "eight point theorem" gives a quick proof of associativity by looking at the intersection of six lines (read down and across) in the following:

$$\left(\begin{array}{c|ccc} & l: & m: & n: \\ \hline r: & P & X & Q+R \\ s: & Q & R & \overline{QR} \\ t: & \overline{PQ} & P+Q & O \end{array}\right)$$

Here, $X = \overline{P(Q+R)} = \overline{R(P+Q)}$ and the eight point theorem is applied to $C_1 : l(X, Y, Z)m(X, Y, Z)n(X, Y, Z) = 0$ and $C_2 : r(X, Y, Z)s(X, Y, Z)t(X, Y, Z) = 0$.

Definition: $Z = 0$ is tangent to PSWF at $[0, 1, 0]$ but the tangent line intersects the curve three times. This is called a *flex point*.

Mordell's Theorem: If a non-singular cubic curve over k has a rational point then the rational points are finitely generated as a k-module. Use $H(\frac{m}{n}) = max(|m|, |n|)$. Let $P = (x, y)$. Define $H(P) = H(x)$ and $h(P) = log(H(P))$. From now on assume C is given by $y^2 = x^3 + ax^2 + bx + c$.

Proof: To prove it, need four lemmas:

Lemma 1: There are a finite number of points P: $h(P) < M$.

Lemma 2: Fix P_0 on C, $\exists K_0(P_0, a, b, c) : h(P + P_0) \leq 2h(P) + k_0$.
Show that if P is on $C(Q)$, $P = (\frac{m}{e^2}, \frac{n}{e^3})$. Then show $n \leq KH(P)^{\frac{3}{2}}$. Use this to get k_0.

Lemma 3: Fix $\exists K(a, b, c) : h(2P) \geq 4h(P) - K$.

Lemma 4: $|\{C(Q) : 2C(Q)\}| < \infty$.

For lemma 4, assume $y^2 = x^3 + ax^2 + bx$ (so the curve always has a rational point), and use $\Gamma = C(Q)$ and $\Delta = 2\Gamma$. Define the map $\phi(x, y) = (x + a + \frac{b}{x}, y\frac{x^2 - b}{x^2})$. Define ψ similarly. Note that $\psi(\phi(P)) = 2P$ and $ker(\phi) = \{0, (0, 0)\}$. Q^{*2} $\alpha(x, y) = x \pmod{Q^{*2}}$. $im(\phi) \subseteq ker(\alpha)$. Let $p_i|b$,

$i = 1, 2, \ldots t$ then $|\Gamma : \phi(\Gamma)| \leq 2^{t+1}$. $|\Gamma : \phi(\Gamma)| \leq 2^{t+1}$. Use the following lemma: If A and B are abelian $A \to B \to A$ and $|B : \phi(A)| < \infty$, $|A : \phi(B)| < \infty$, then $|A : 2A| \leq |B : \phi(A)||A : \phi(B)|$.

Proof given lemmas: Let $Q_0, \ldots, Q_{m-1}$ be the coset representatives. $P - Q_{i_1} = 2P_1$ is in the subgroup, $P_1 - Q_{i_2} = 2P_2$, repeatedly doing this yields: $P = Q_{i_1} + 2Qi_2 + \ldots + 2^{m-1}Q_{i_m} + 2^m P_m$, $h(P_j) \leq \frac{3}{4}h(P_{j-1})$. Since there are a finite number of Q_i there's a k' so that $h(P - Q_i) \leq 2h(P) + k'$ for all P. Using the inequalities $h(P_j) \leq \frac{h(P_{j-1})}{2} + \frac{k+k'}{4}$. So the group is generated by the Q_i and the (finite number of) points of $ht \leq \frac{k+k'}{4}$.

Theorem: Let C be a non-singular cubic curve $C : y^2 = x^3 + ax^2 + bx + c$. Set $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$. Let Φ be the set of points of finite order. Let ϕ be the reduction map mod p. If $(p, 2D) = 1$ then ϕ is an injection into $C(F_p)$.

Nagel-Lutz Theorem: Same as above with $P(x, y)$ as a rational point of finite order $y = 0$ or $y|d^2$.

Functions on Elliptic Curves: $f_1(x, y) = \frac{s(x,y)}{t(x,y)}$ and $f_2(x, y) = \frac{u(x,y)}{v(x,y)}$ are said to be *equivalent* on the elliptic curve E, denoted by $f_1 \sim_E f_2$ iff $(sv - ut) = 0 \,(\text{mod } E)$. Polynomials can be uniquely x or y reduced but not rational functions. *Examples:* Let $E : y^2 - (x^3 + x^2 + x)$ then $\frac{x}{y-x} \sim_E \frac{y+x}{x^2+1}$. Put $F(X, Y, Z) = \{\frac{x}{y}\} = [X, Y]$ then $F[0, 1, 0] = [0, 1] \sim_E 0$ (a zero) while if $G(X, Y, Z) = \{\frac{y}{x}\} = [Y, X]$ then $G[0, 1, 0] = [0, 1] \sim_E \infty$. For $E : y^2 = x^3 - x$, $\{\frac{y}{x^2-1}\} \sim_E \{\frac{x}{y}\}$ and $[YZ, X^2 - Z^2] \sim_E [X, Y]$. For $E : y^2 = x^3 - x$, $\{x\}$ has a 0 at $(0, 0)$, $\{y\}$ has a 0 at $(-1, 0), (0, 0), (1, 0)$, $\{\frac{x}{y}\}$ has a 0 at $(-1, 0), (1, 0)$. If $E(a, b)$ is non-singular, E is irreducible and we can embed $k[x, y]/(E)$ in the field of fractions $K(E)$ and we can define a map from $K(R) \to \overline{K} \cup \{\infty\}$.

Definition: A *morphism* between two elliptic curves C_1 and C_2 is a rational map $\varphi : (C_1, I_1) \to (C_2, I_2)$, $\varphi(x, y) = (f(x, y), g(x, y)), g, g \in K(C_1)$, such that $\varphi(P + Q) = \varphi(P) + \varphi(Q)$. $\varphi(P) = [n]P$ is a morphism. A morphism is an *isomorphism* if $\exists\psi$, a morphism: $\psi \circ \varphi = [1]$. An *isogony* is a surjective morphism with finite kernel preserving the base point. If $\psi : E_1 \to E_2$ induces a $\psi^* : K(E_2) \to K(E_1)$. $\psi^*(f) = f \circ \psi$. $deg(\psi) = ker(\psi)$.

Example of dual isogony: $E : y^2 = x^3 + x^2 + x$, $E' : (y')^2 = (x')^3 - 2(x')^2 - 3(x')$. $\psi(x, y) = (\frac{y^2}{x^2}, \frac{y(1-x^2)}{x^2})$, $\varphi(x', y') = (\frac{(y')^2}{4(x')^2}, \frac{(y')(-3-(x')^2)}{8(x')^2},)$ and $\varphi \circ \psi = [2]$.

Definition: Suppose $E = E_{a,b}(K), char(K) \neq 2, 3$. Let $x_1 = \mu^2 x$ and $y_1 = \mu^3 y$ then $(x_1, y_1) \in E_{a',b'}(K)$ with $a' = \mu^4 a$ and $b' = \mu^6 b$. Two elliptic curves related in this way are said to be *isomorphic*.

Theorem: If $K = F_{p^m}, p \neq 2, 3$ and $E_K^{(1)}(a, b) \cong E_K^{(2)}(\overline{a}, \overline{b})$ iff $\exists u \in K^*$ such that $u^4\overline{a} = a$ and $u^6\overline{b} = b$ under the map $(x, y) \mapsto (u^2x, u^3y)$.

Definition: $j(E) = 1728\frac{4a^3}{4a^3+27b^2}$ is called the *j-invariant*.

Theorem: $j(E)$ is invariant under the transformation above (i.e. - two isomorphic curves have the same j-invariant) and, conversely, two curves with the same j value are related in this way (and are thus isomorphic in the elliptic curve defined over the algebraic closure).

Theorem: If $j(E_1) = j(E_2)$ then $\exists \mu \in \overline{K}, \mu \neq 0 : a_2 = \mu^4 a_1, b_2 = \mu^6 b_2$.

Homogeneous forms: Let $G(u,v)$ be a homogeneous polynomial and $(u_0, v_0) \in \mathbb{P}^1_K$, $\exists k \geq 0$ and $H(u,v)$ with $H(u_0,v_0) \neq 0 : G(u,v) = (v_0 u - u_0 v)^k H(u,v)$. Any line in $\mathbb{P}^2_k$ can be parameterized by $(x,y,z) = (a_0 u + b_0 v, a_1 u + b_1 v, a_2 u + b_2 v)$. L intersects C to order n at $P = (x_0 : y_0 : z_0)$ if $\overline{C}(u,v) = (v_0 u - u_0 v)^n H(u,v)$ in the foregoing theorem; denote this as $ord_{L,P}(C) = n$, $ord_{L,P}(C) = \infty$ if $\overline{C}$ is identically 0. If L_1, L_2 are lines, $ord_{L_1,P}(P) = 1$ or ∞. If C is a curve defined by $C(x,y,z) = 0$, C is non singular at P if $(C_x, C_y, C_z) \neq 0$ in which case the tangent line is $C_x X + C_y Y + C_z Z = 0$. If C is non-singular at P there is a line in $\mathbb{P}^2_K$ that intersect C to order at least 2.

Theorem: The number of equivalence classes of elliptic curves over K is $2q+6$, $2q+2$, $2q+4$, $2q$ according to $q = 1, 5, 7, 11 \pmod{12}$. If $K = F_{2^m}$ and $E_K(a,b) : y^2 + xy = x^3 + ax^2 + b$ then $E^{(1)}_K(a,b) \cong E^{(2)}_K(\overline{a}, \overline{b})$ iff $b = \overline{b}, Tr(a) = Tr(\overline{a})$ and if so $\exists s : \overline{a} = s^2 + s + a$ under the map $(x,y) \mapsto (x, y + sx)$.

Division Polynomials: Let $E(K) : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ be an elliptic curve $m \in \mathbb{Z}, P = (x,y)$, $b_2 = a_1^2 + 4a_2$, $b_4 = a_1 a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$, $b_8 = a_1^2 a_6 + 2a_4 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$ then $\exists \psi_m(x,y), \omega_m(x,y), \theta_m(x,y) \in K[x,y]$ such that $[m]P = (\frac{\theta_m(x,y)}{(\psi_m(x,y))^2}, \frac{\omega_m(x,y)}{(\psi_m(x,y))^3})$. $\psi_1 = 0$, $\psi_1 = 2$, $\psi_2 = 2y + a_1 x + a_3$, $\psi_3 = 3x^4 + b_2 x^2 + 3b_4 x^2 + 3b_6 + b_8$, $\psi_4 = (2x^6 + b_2 x^5 + 5b_4 x^4 + 10 b_8 x^2 + (b_2 b_8 - b_4 b_6)x + b_4 b_8 - b_6^2)\psi_2$, $\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, m \geq 2$, $\psi_{2m} = \frac{\psi_m}{\psi_2}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$, $\theta_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}$, $\omega_m = \frac{1}{4y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), m > 2$. Note that $deg(\psi_m) = O(m^2)$.

Definition: An *endomorphism* is a homomorphic map between and an elliptic curve and itself that is expressible as a *rational function.* If α is an endomorphism and $P = (x,y), \alpha(X+Y) = \alpha(X) + \alpha(Y), \alpha(x,y) = (r_1(x,y), r_2(x,y))$. Because $y^2 = x^3 + ax + b$, we may assume $\alpha(x,y) = (r_1(x), y r_2(x))$; if $r_1(x) = \frac{p(x)}{q(x)}$, the degree of endomorphism is $max(deg(p(x)), deg(q(x)))$. This endomorphism α is a *separable endomorphism* if $r_1'(x) \neq 0$. The *Frobenius endomorphism* is $\varphi(x,y) = (x^q, y^q)$.

Definition: $E[n] = \{P \in E(\overline{K}) : nP = \infty\}$.

Theorem: (1) If $char(K) \neq 2$ $E[2] = \mathbb{Z}_2 \oplus \mathbb{Z}_2$; if $char(K) = 2$ $E[2] = \mathbb{Z}_2$ or 0. (2) If $char(K) \nmid n$ or is 0, $E[n] = \mathbb{Z}_n \oplus \mathbb{Z}_n$. (3) If $char(K) = p \mid n, n = p^r n'$ then $E[n] = \mathbb{Z}_n \oplus \mathbb{Z}_{n'}$ or $E[n] = \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'}$. Proof uses division polynomials. Let E be an elliptic curve over F_q. Then $E(F_q) = \mathbb{Z}_n$ or $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ with $n_1 \mid n_2$.

> *Proof:* Apply the above theorem. ϕ_n induces a linear transformation on $E[n]$. $E[n] = Z_{n_1} \oplus \ldots \oplus Z_{n_k}$ by ther FTOAG. Let $l \mid n_1$ so $l \mid n_j$. $E[l] \subseteq E[n]$, so it has order l^k. But the endomorphism induced by multiplication by n has order n^2, so $k = 2$. Since this map, annihilates $Z_{n_1} \oplus Z_{n_2}$, $n_1, n_2 \mid n$, and since $n^2 = \#E[n]$, $n_1 = n_2 = n$.

Theorem: If α be a separable endomorphism of $E_{A,B}(\overline{F_q})$, $deg((\alpha) = |ker(\alpha)|$, otherwise $deg((\alpha) > |ker(\alpha)|$.

> *Proof:* $\alpha(x,y) = (r_1(x), y r_2(x))$, $r_1(x) = \frac{p(x)}{q(x)}$; since α is separable, $p'q - q'p \neq 0$. Let $S = \{x \in \overline{K} : (pq' - qp')q = 0\}$. There are (a,b) on the curve: $a \neq 0 \neq b$, $(a,b) \neq O$. $deg(p - aq) = deg(\alpha)$, and $a \notin r_1(S)$. There are exactly $deg(\alpha)$ points: $\alpha(x,y) = (a,b)$. STS there are no nultiple roots. If x_0 is a multiple root, $pq' - qp'(x_0) = 0$. If α is not separable, the same argument holds but the equation has at least one solution with multiple roots so it has fewer roots than $deg(\alpha)$.

Theorem: $\alpha : E_{A,B}(\overline{K}) \to E_{A,B}(\overline{K})$ is surjective.

Proof: If $p - aq$ is not constant and x_0 is a root, $q(x_0) \neq 0$. Choose $y_0^2 = x_0^3 + Ax_0 + B$. $\alpha(x_0, y_0) = (a, b')$, $b' = \pm b$. If $b' = b$, we're done. If $\alpha(x_0, y_0) = (a, -b') = (a, b)$. Since $E(\overline{K})$ is infinite and $ker(\alpha)$ is finite, only a finite number of points map onto a points with a single x coordinate. Therefore either p or q is not constant. There is a unique a such that $p - aq$ is constant. So there are at most two points, namely, $(a, \pm b)$ not in the image. Pick another P_1: $\alpha(P_1) = (a_1, b_1)$. $(a_1, b_1) + (a, b) \neq (a, \pm b)$. There is a unique P_2: $\alpha(P_2) = (a_1, b_1) + (a, b)$ so $\alpha(P_2 - P_1) = (a, b)$ and $\alpha(P_1 - P_2) = (a, -b)$.

Theorem: $\phi_q^n - 1$ is separable and $|ker(\phi_q^n - 1)| = |\#E(F_q)|$.

Proof: ϕ is a homomorphism. It has degree q and $(x^q)' = 0$.

Theorem: Let $E_{A,B}$ be an elliptic curve. Fix $(u, v) \in E$. Define $f(x, y), g(x, y)) = (x, y) + (u, v)$. Then $\frac{\frac{df(x,y)}{dx}}{g(x,y)} = \frac{1}{y}$.

Use the addition formula and the fact that $2yy' = 3x^2 + A$ to get $(x - u)^3 u(\frac{df(x,y)}{dx} - g(x, y)) = v(Au + u^3 + v^3 - Ax - x^3 - y^2) + y(-Au - u^3 - v^3 + Ax + x^3 - y^2)$. Now use $B = y^2 - x^3 - Ax$ to get the result.

Theorem: Let $\alpha_i, i = 1, 2, 3$ be endomorphisms. Write $\alpha_i(x, y) = (R_{\alpha_i}, S_{\alpha_i} y)$. Suppose $\exists c_{\alpha_1}, c_{\alpha_2} : \frac{R'_{\alpha_i}}{S_{\alpha_i}} = c_{\alpha_i}, i = 1, 2$. Then $\frac{R'_{\alpha_3}}{S_{\alpha_3}} = c_{\alpha_1} + c_{\alpha_2}$.

Proof: $\frac{\partial x_3}{\partial x_1} = \frac{y_3}{y_1}$ and $\frac{\partial x_3}{\partial x_2} = \frac{y_3}{y_2}$. $\frac{\partial x_j}{\partial x} = c_{\alpha_j} \frac{y_j}{y}$. Now apply the chain rule.

Theorem: Let $E_{A,B}$ be an elliptic curve, $n \in \mathbb{Z}$ and $n(x, y) = (R_n(x), yS_n(x))$. Then $\frac{R'_n}{S'_n} = n$.

Proof: From the inverse formula if it holds for $n > 0$, it holds for $n < 0$. It holds for $n = 1$ and the result above shows if it holds for n, it holds for $n + 1$.

Theorem: $r, s \in \mathbb{Z}$, $r \neq 0 \neq s$ then $r\phi_n + s$ is separable iff $p \nmid s$. $(x, y) \in E(F_q)$ iff $\phi_p(x, y) = (x, y)$.

Proof: $r(x, y) = (R_r(x), yS_r(x))$. $(R_{r\phi_q(x)}(x), y_{r\phi_q}(x)) = (R_r^q, y(x^3 + Ax + B)^{\frac{q-1}{2}} S_r^q(x))$. Thus $c_{r\phi_q} = R'_{r\phi_q}/S_{r\phi_q} = 0$. $R_{r\phi_q+s}/S_{r\phi_1+s} = c_{r\phi_q} + c_s = s \neq 0 \pmod{p}$.

Theorem: $deg(a\alpha + b\beta) = a^2 deg(\alpha) + b^2 deg(\beta) + ab(deg(\alpha + \beta) - deg(\alpha) - deg(\beta)$.

Proof: Consider α_n and β_n given by the matricies when viewed as maps in $E[n]$. The matrix calculation is straigntforward.

Theorem: Let E be an elliptic curve over K and n a positive integer, $char(K) \nmid n$. There is a pairing $e_n : E[n] \times E[n] \to \mu_n$ (the Weil pairing) with (1) e_n bilinear in each variable, (2) e_n, non-degenerate, (3) $e_n(T, T) = 1$, (4) $e_n(T, S) = e(S, T)^{-1}$, $e_n(\sigma T, \sigma S)$ for $\sigma \in Aut(\overline{K})$, and (6) $e_n(\alpha(S), \alpha(T)) = e_n(s, T)^{deg(\alpha)}$, for all seperable automorphisms of E. If the coefficients are in F_q, the statement holds for ϕ_p.

Proof: The proof uses divisor theory.

Theorem: Let $\{T_1, T_2\}$ be a basis in $E[n]$. Then $e_n(T_1, T_2)$ is a primitive n-th root of unity.

Proof: Suppose $e_n(T_1, T_2) = \zeta$, $zeta^d = 1$. $e_n(T_1, dT_2) = 1$ and $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$. Let $S = aT_1 + bT_2$. $e_n(T_1, dT_2) = e_n(T_1, dT_2)^a e_n(T_t, dT_2)^b = 1$. This is true for all S so $dT_2 = \infty$. But this can hold iff $n \mid d$, so ζ is a primitive root.

Theorem: Let α be and endomorphism of E over K and n, a positive integer not divisible by $char(K)$. Then $deg(\alpha_n) = deg(\alpha) \pmod n$.

Proof: By the previous result, $\zeta = e_n(T_1, T_2)$ is primitive. So $\zeta^{deg(\alpha)} = e_n(T_1, T_2) = e_n(aT_1 + cT_2, bT_1 + dT_2) = \zeta^{ad-bc}$.

Theorem: $r, s \in \mathbb{Z}$, $(r, q) \neq 1$ then $deg(r\phi_n - s) = r^2q + s^2 - rsa$, where $a = q + 1 - \#E(F_q)$.

Proof: $deg(r\phi_q - s) = r^2 deg(\phi_q) + s^2 deg(-1) + r(deg(\phi_q - 1) - deg(\phi_q) - deg(-1))$.

Theorem: $a = q + 1 - \#E(F_q)$. $\phi_q^2 - a\phi_q + q = 0$ and $a = Tr((\phi)_q)_m \pmod m$.

Proof: Consider $\alpha = \phi_q^2 - a\phi_q + q$ as an endomophism in $E[m]$. $|ker(\phi_q - 1)| = deg(\phi_q - 1) = det((\phi_q)_m - I)$. By Cayley Hamilton, $(\phi_q^2)_m - a\phi_q + q = 0 \pmod m$. This is true for infinitely many m so $\alpha = 0$.

Hasse's Theorem: Let E_q be an elliptic curve then $q + 1 - 2\sqrt{q} \leq \#E_q \leq q + 1 + 2\sqrt{q}$, $\#E_q = q + 2 - t$, t is the Frobenius trace.

Proof of Hasse: Let ψ be the Frobenius map. $\#E_p = |ker([1]-\psi)|$. First note that $deg([1]) = 1$ (in fact, $deg([n]) = n^2$). $deg(\psi) = p$. Also note that $deg(a+b) - deg(a) - deg(b) = B(a, b)$ is bilinear. $0 \leq deg([t] + [2]\psi) = t^2 - 4p - 2tB[1, -\psi] = 4p - t^2$; so $(deg([1] - \psi) - deg([1]) - deg(\psi))^2 \leq 4p$ but the first term is $\#E(F_p)$.

Theorem: If $\alpha \neq 0$ is a separable endomorphism of E, $deg(\alpha) = \#ker(\alpha)$, otherwise $deg(\alpha) > \#ker(\alpha)$. The endomorphism $[n]P \mapsto Q$ has degree n^2; most endomorphisms are of this form. If $char(K) \nmid n$ then $E[n] = \mathbb{Z}_n \oplus \mathbb{Z}_n$. If $E[n] \subseteq E(\mathbb{K})$ then $\mu_n \in K$. Given $E_q(a, b), n \geq 1$, (1) $ker(\phi_q^n - 1) = \#E_{q^n}(a, b)$ and $\phi_q^n - 1$ is separable $\#E_{q^n}(a, b) = deg(\phi_q^n - 1)$. If α is separable, then $deg(\alpha) = \#ker(\alpha)$. $|E(\overline{F_p})[m]| = m^2$ if $(m, p) = 1$.

Theorem: Let $E(F_q)$ be an elliptic curve $E(F_q) \approx \mathbb{Z}_n$ or $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}, n_1 \mid n_2$. The Frobenius endomorphism has degree q and is not separable.

Definitions: If E_q is an elliptic curve over a finite field of characteristic p, E_q is said to be *supersingular* if $E_q[p] = \{\infty\}$. (1) $char(F) \neq 2, 3$, $(x, y) \mapsto (\frac{x-3a_1^2-12a_2}{36}, \frac{y-3a_1x}{216} - \frac{a_1^3+4a_aa_2-12a_3}{24})$, sends the general equation to $E_q(a, b) : y^2 = x^3 + ax + b, \Delta = -16(4a^3 + 27b^2)$. (2) $char(F) = 2, a_1 \neq 0$, $(x, y) \mapsto (a_1^2x + \frac{a_3}{a_1}, y + \frac{a_1^2a_4-a_3^2}{a_1^2})$, sends the general equation to $E_q(a, b) : y^2 + xy = x^3 + ax + b, \Delta = b$. This is *non-supersingular.* (3) $char(F) = 2, a_1 = 0$, $(x, y) \mapsto (x + a_2, y)$, sends the general equation to $E_q(a, b) : y^2 + cy = x^3 + ax + b, \Delta = c^4$. This is supersingular. (4) $char(F) = 3, a_1^2 \neq -a_2$, $(x, y) \mapsto (x + \frac{d_4}{d_2}, y + a_1x + a_1\frac{d_4}{d_2} + a_3)$, $d_2 = a_1^2 + a_2, d_4 = a_4 - a_1a_3$, sends the general equation to $E_q(a, b) : y^2 = x^3 + ax + b, \Delta = -a^3b$. This is non-supersingular. (5) $char(F) = 3, a_1^2 = -a_2$, $(x, y) \mapsto (x, y + a_1x + a_3)$, sends the general equation to $E_q(a, b) : y^2 = x^3 + ax + b, \Delta = -a^3$. This is supersingular.

Theorem: $q = p^m$, $\exists E_q : \#E_q = q + 1 - t$ iff (i) $t \neq 0(p), t^2 \leq 4q$; or, (ii) $m = 1(2)$ and either (a) $t = 0$ or (b) $t^2 = 2q, p = 2$, or (c) $t^2 = 3q, p = 3$; or, (iii) $m = 0(2)$ and either (a) $t^2 = 4q$ or (b) $t^2 = q, p \neq 1(3)$ or (c) $t = 0, p \neq 1(4)$. E_{p^m} is supersingular iff $p \mid t$. $E_q = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ and $n_2 \mid n_1 \mid (q - 1)$.

Divisors: Given $E(K)$, $P \in E(\overline{K})$, define $D = \sum_j a_j[P_j], a_j \in \mathbb{Z}$ and $deg(D) = \sum_j a_j$. $Div^0(E)$ are the *divisors* of degree 0. If f is a function on E, $div(f) = \sum_P ord_P(f)[P] \in div(E)$. Two divisors D_1, D_2 are said to be *equivalent* if $D_1 - D_2 = (D)_E$.

Theorem: If $P - Q$ is a divisor on an elliptic curve E, $P - Q = c$. The theorem can be applied as follows. Suppose $div(\{f\}) = P_1 + P_2 + \ldots + P_n Q_1 - Q_2 - \ldots - Q_n$. Let l_1 be the line through P_1, P_2 and hence $-(P_1 + P_2)$ while m_1 is the line through $-(P_1 + P_2)$ and O and hence $P_1 + P_2$ then $div(\{f\}\frac{m_1}{l_1}) = (P_1 + P_2) + \ldots + P_n + O - Q_1 - \ldots - Q_n$ continuing and doing the same for the Q_i, we get $div(\{f\} \cdot \frac{m_1}{l_1} \cdot \frac{m_2}{l_2} \cdot \ldots \frac{m_{2n-2}}{l_{2n-2}}) = (P_1 + P_2 + \ldots + P_n) + (n-1)O - (Q_1 + \ldots + Q_n) - (n-1)O = (P_1 + P_2 + \ldots + P_n) - (Q_1 + \ldots + Q_n)$ so $f = c(\frac{l_1}{m_1} \cdot \frac{l_2}{m_2} \cdot \ldots \frac{l_{2n-2}}{m_{2n-2}})$ by the theorem.

Example of divisor calculations: $div(\{x\}) = 2(0,0) - 2\infty$, $div(\{y\}) = (-1,0) + (0,0) + (1,0) - 3\infty$, $div(\{\frac{x}{y}\}) = (0,0) + \infty - (-1,0) - (1,0)$. Let $E : y^2 = x^3 - 2x - 5$ and $D = (2,3) + (2,-3) + O - 2(-2,1) - (29,156)$. We can confirm $(2,3) + (2,-3) + O = O$ and $2(-2,1) + (29,156) = O$ are elliptic curve divisors. The line containing $(2,3), (2,-3), O$ is $x - 2 = 0$. The line containing $2(-2,1)$ and $(25,156)$ is $y - 5x - 11 = 0$, so $div(\frac{x-2}{y-5x-11}) = D$.

Theorem: $D = \sum_P n_P P$ is a divisor of an elliptic curve E iff $\sum_P n_P = 0$ and $\sum_P [n_P]P = 0$.

Definition: $f \circ n(P) = f(nP)$. If $T \in E[n], \exists T' \in E[n^2] : nT' = T$ and $g = f \circ n, div(g) = \sum_{R \in E[n]} [T' + R] - [R]$. $g(P+S)^n = g(P)^n$ so $(\frac{g(P+S)}{g(P)})^n = 1$. Define the *Weil pairing* as $e_n(S,T) = \frac{g(P+S)}{g(P)}$. If σ is an automorphism, $e_n(\sigma S, \sigma T) = \sigma e_n(S,T)$. If α is separable, $e_n(\alpha S, \alpha T) = e_n(S,T)^{deg(\alpha)}$.

Theorem (Siegal): An elliptic curve over $\mathbb{Q}$ has only finitely many integer points.

Theorem (Mazur): The set of torsion points $T_E(\mathbb{Q})$ of $E/\mathbb{Q}$ is one of $\mathbb{Z}/n\mathbb{Z}, n = 1, 2, \ldots, 10, 12$ or $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, $n = 1, 2, 3, 4$.

Theorem: For every isogony $\psi : E \to E'$ there is a *dual* $\hat{\psi} : \hat{\psi}\psi = [2]_E$. $Frob_n : \overline{F_p} \to \overline{F_p}$ and $F_{p^n} = \{\alpha \in \overline{F_p} : Frob_n(\alpha) = \alpha\}$.

Theorem: $\#E(F_p) = p + 1 + \sum_{x=0}^{p-1}(\frac{x^3+ax+b}{p})$.

Point Counting: Counting points by baby-step giant-step is $(O(q^{\frac{1}{4}+\epsilon}))$. Set $N = \#E_q$ then $q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}$; if $[m]P = \infty$ then $N = m$, probably. Put $m = q + 1 - 2\sqrt{q} + k, l = \lceil \sqrt{4}\sqrt{q} \rceil, k = al + b$, then $[m]P = [c]P + [a]S + [b]P, c = q + 1 - 2\sqrt{q}, S = [l]P$ or $[c]P + [a]S = -[b]P$. Baby step computes LHS and stores it. Giant step computes RHS and does a lookup.

Schoof point counting: Let φ be the Frobenius automorphism $\varphi(x,y) = (x^q, y^q)$. Schoof calculates

$t \pmod l$ for a set of primes $l \in \mathcal{P}$ with $\prod_{l \in \mathcal{P}} l > 4\sqrt{q}$ and then construct t using CRT finally returning $q + 1 - t$. Here's how:

(1) For $l = 2$, $t = 0 \pmod l$ iff $(x^3 + ax + b, x^q - x) \neq 1$.

(2) if l is odd, set $q_l = q \pmod l, |q_l| < \frac{l}{2}$; find $(x', y') = \varphi(x, y)^2 + q_l(x, y) \pmod{\psi_l(x, y)})$; for $j = 1, 2, \ldots \frac{l-1}{2}$:

(i) Compute $(x_j, y_j) = j(x, y)$;

(ii) if $x' - x_j^q = 0 \pmod{\psi_l}$, go to iii, if not, try next j, if all such j's have been tried, go to (iv);

(iii) Compute y', y_j, if $\frac{y' - y_j}{y} = 0 \pmod{\psi_l}$ then $t = j \pmod l$ otherwise $t = -j \pmod l$;

(iv) Let $w^2 = q \pmod l$, if no such w exists, $t = 0 \pmod l$;

(v) if $(x^q - x_w, \psi_l) = 1$ then $t = 0 \pmod l$, otherwise, set $g = numerator(\frac{y^q - y_w}{y}, \psi_l)$, if $g \neq 1$, $t = 2w \pmod l$ otherwise $t = -2w \pmod l$.

Definition of Complex Multiplication: $E : y^2 = x^3 - x$, $\mu : E \to E$, $\mu(x, y) = (-x, iy)$, $\mu^2 = [-1]$.

Definition: If $D = \sum_{P \in E} n_P[P]$, $deg(D) = \sum_P n_P$ and $sum(D) = \sum_P n_P P$. $div(f) = \sum_{P \in E(\overline{K})} ord_P(f)[P] \in Div(E)$.

Theorem: Let E be an elliptic curve and f be a function on E not 0 then (1) f has finitely many poles and zeros, (2) $deg(div(f)) = 0$ and (3) if there are no poles or zeros, f is a constant.

Theorem: Let E be an elliptic curve and D a divisor on E with $deg(D) = 0$ then $\exists f$ on E with $div(f) = D, sum(D) = \infty$.

Pairing: $e_n : E[n] \times E[n] \to \mu_n$. μ_n is the nth roots of unity.

Definition: For simplified case of elliptic curves in Weierstrauss form ($E : y^2 = x^3 + Ax + B$), all polynomials, $f(x, y)$, on E, denoted $f \in K[E]$, can reduced to normal form, $f(x, y) = v(x) + yw(x)$. If $f(x, y) = v(x) + yw(x)$, $\overline{f} = v(x) - yw(x)$ and $N(f) = f\overline{f}$. $deg(f) = \max(2deg_x(v), 3 + 2deg_x(w))$.

Theorem: If $f \in K[E]$ then $deg(f) = deg_x(N(f))$ and $deg(f)$ has the usual properties.

Theorem: If $r \in K(E)$ and $P \in E$, $\exists u \in K(E)$ such that (1) $u(P) = 0$ and (2) if $r \in K(E)$, $\exists s \in K(E)$: $r = u^d s$. Further, d does not depend on the choice of u.

Proof: For the SWF curve, we can specify u as follows: (1) For $P = (a, b) \in E, b \neq 0$, $u(x, y) = (x - a)$; (2) For $P = (w, 0) \in E$, $u(x, y) = y$; and (3) For $P = \infty$, $u(x, y) = \frac{x}{y}$.

Definition: For the notation of the previous theorem, define $ord_P(r) = d$.

Theorem: Let $r \in K(E)$, $\sum_P ord_P(r) = 0$. If $f \in K[E]$ then the sum of the multiplicities of the zeros of f equals the degree of f.

Definition: $\Delta \in Div(E)$ is principal if $\Delta = div(r)$ for some $r \in K(E)$. The principal divisors are denoted $Prin(E)$ and $Pic(E) = Div(E)/Prin(E)$. $|\Delta| = \sum_{P \in P-\infty} |m(P)|$.

Theorem: Let $\Delta \in Div(E), \exists \tilde{\Delta} \in Div(E)$ with $\Delta \sim \tilde{\Delta}$ with $deg(\Delta) = deg(\tilde{\Delta})$ and $|\tilde{\Delta}| \leq 1$.

Theorem: $\forall \Delta \in Div^0(E), \exists! P \in E$: $\Delta \sim \langle P \rangle - \langle \infty \rangle$.

Theorem: Let $[n] : E \to E$ be represented by the rational function $[n](P) = (g_n(P), h_n(P))$ then if $(n, p) = 1$, $\frac{g_n}{x}(O) \sim \frac{1}{n^2}$ and $\frac{h_n}{y}(O) \sim \frac{1}{n^3}$.

Theorem: Let $P, Q \in E$ and suppose u is a uniformizing parameter at P, define $T_Q(u)](R) = u(R + Q)$ then $T_Q(u)$ is the uniformizing parameter at $P - Q$.

Theorem: Let E be an elliptic curve with $deg(D) = 0$. $\exists f \in K(E) : D = div(f)$ iff $sum(D) = \infty$.

Theorem: Suppose $m > n > 0$ and $m, n, m-n, m+n$ are all prime to p, then $div(g_m - g_n) = \langle E[m+n] \rangle + \langle E[m-n] \rangle - \langle E[m] \rangle - \langle E[n] \rangle$. If $(n, p) = 1$, $|E[n]| = n^2$.

Theorem: If $(n, p) = 1$, $div(\phi_n) = \langle E[n] \rangle - n^2 \langle \infty \rangle$.

Theorem: Suppose $r \in K(E)$ is a non-constant function, then r takes on all values including ∞.

Theorem: Suppose $f : E \to E, K(E)$ is a non-constant then f is onto.

Definition: The *ramification index* of F at P is defined by $e_F(P) = ord_P(u \circ F)$.

Theorem: $ord_P(u \circ F) = ord_{F(P)}(r) \cdot e_F(P)$.

Definition: $F^* : Div(E) \to Div(E)$ is $F^*(\langle Q \rangle) = \sum_{F(P)=Q} e_F(P) \langle P \rangle$.

Theorem: F^* is 1-1, $div(r \circ F) = F^*(div(r))$ and $e_{F_1 \circ F_2}(P) = e_{F_1}(F_2(P)) \cdot e_{F_2}(P)$.

Theorem: Suppose $\alpha : E \to E$ is a non-zero endomorphism then $e_\alpha(P)$ is independent of P.

For $m \in \mathbb{Z}, r \in K(E)$ with D the derivative then $D(r \circ [m]) = (m \circ D(r)) \circ [m]$.

Theorem: If φ is the Frobenius homomorphism over $GF(q)$ then $e_\varphi = q$.

Definition: $e_\alpha = 1$ means α is separable.

Theorem: If $(m, p) = 1$ then $[m]$ is separable.

Theorem: If $(m, p) = 1$ and $(n, p) = 1$ then $[m] + [n]\varphi$ is separable.

Theorem: If $P \in E[m]$ then $[m]^*(\langle T \rangle - \langle \infty \rangle)$ is principal.

Definition: A rational map $F : E \to E'$ that is a group homomorphism from E into E' is a *morphism.*

Theorem: Let T_1 and T_2 be a basis for $E[m]$ then $e + m(T_1, T_2)$ is a primitive m-th root of unity.

Definition: If α is an endomorphism then $\alpha(E[m]) \subseteq E[m]$

Definition: Let M be an algebraic extension of L and A_r is the linear map from M to M represented by multiplication by r with respect to the basis $r_1, \ldots, r_n$ and $f_r(x) = det(xI - A_r)$ with constant term $c_n = (-1)^n det(A_r)$. Define $N(r) = det(A_r)$.

Definition: Suppose $\alpha : E \to E'$ be an isogony $K' = \alpha^*(K(E')) \subseteq K(E)$. Define $N = N_{K(E)/K'}$ then $N(r)](P) = \prod_{\alpha(Q)=\alpha(P)} r(Q)^{e_\alpha}$.

Definition: Let $r \in K(E)$ and $D \in Div(E)$. Suppose $div(r)$ and D have disjoint support define $r(D) = \prod_{P \in E} f(P)^{n_p}$. For $f, g \in K(E)$ further define $\langle f, g \rangle_P = (-1)^{mn}[\frac{f^n}{g^m}](P)$ where $m = ord_P(f)$ and $n = ord_P(g)$. $\langle f, g \rangle_P$ is called the local symbol of f and g.

Weil Reciprocity Theorem: $\prod_{P \in E} \langle f, g \rangle_P = 1$.

Construction of the Weil Pairing: For $T \in E[n], \exists f : div(f) = n[T] - n[\infty]$. Choose $T' \in E[n^2] : nT' = T$ then $\exists g : div(g) = \sum_{R \in E[n]}([T' + R] - [R])$. Put $f \circ n(P) = f(nP)$. This gives $f \circ n(P) = g^n(P)$. Put $e_n(S, T) = \frac{g(P+S)}{g(P)} \in \mu_n, S \in E[n], P \in E(\overline{K})$ and e_n satisfies the pairing properties.

Example: If $E(F_7) : y^2 = x^3 + 2$ then $E(F_7)[3] = \mathbb{Z}_3 \oplus \mathbb{Z}_3$. To compute $e_3((0,3),(5,1))$, $D_{(0,3)} = [(0,3)] - [\infty]$ and $D_{(5,1)} = [(3,6)] - [(6,1)]$, $div(y-3) = 3D_{(0,3)}$ and $div(\frac{4x-y+1}{5x-y-1}) = 3D_{(5,1)}$. $f_{(0,3)}(D_{(5,1)}) = \frac{f_{(0,3)}(3,6)}{f_{(0,3)}(6,1)} = \frac{6-3}{1-3} = 2 \pmod 7$. $f_{(5,1)}(D_{(0,3)}) = 4$, $e_3((0,3),(5,1)) = \frac{4}{2} = 2 \pmod 7$.

Theorem: If $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ $E(F) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$; if $F = \mathbb{F}_p, p \nmid m, \exists k : E(F_{p^k}) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Note: If $m[P] = O$, $m[P] - m[O]$ is a divisor of $E(F)$.

Theorem: Let $P, Q \in E[m]$, $div(f_P) = m[P] = m[O]$, $div(f_Q) = m[Q] = m[O]$ then $e_m(P,Q) = \frac{f_P(Q+S)}{f_P(S)} / \frac{f_Q(P-S)}{f_Q(-S)}$ for $S \in E(F)$ is bilinear. $E[m] = \langle aP_1 + bP_2 \rangle$ and suppose. $P = a_P P_1 + b_P P_2 \rangle$, $e_m(P,Q) = \zeta^{det\begin{pmatrix} a_P & a_Q \\ b_P & b_Q \end{pmatrix}}$ where $\zeta = e_m(P_1, P_2)$.

Theorem (for Miller's Algorithm): Let E be an elliptic curve and $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ are non-zero points on E. Let λ the the slope of the line betwween P and Q and define $g_{P,Q} = x - x_P$ if $\lambda = \infty$ and $g_{P,Q} = \frac{y - y_p - \lambda(x - x_P)}{x + x_P + x_Q + \lambda^2}$, otherwise. Then (a) $div(g_{P,Q}) = [P] + [Q] - [P+Q] - [O]$ and (b) For $m \geq 1$ with binary representation $[m_{n-1}, \ldots, m_0]$ satisfies $div(f_P) = m[P] - [mP] - (m-1)[O]$ where $g_{T,T}$ and $g_{T,P}$ are defined by Miller's algorithm.

Miller's Algorithm:

1. Set $T = P$ and $f = 1$;
2. for$(i = (n-2); i \geq 0; i--)$
    3. $f = f^2 \cdot g_{T,T}$;
    4. $T = 2T$;
    5. if$(m_i = 1)$
        6. $f = f \cdot g_{T,P}$;
        7. $T = T + P$;
8. $return(f)$.

Definition: Let $P, Q \in E(F_q)[l]$, choose $f_P : div(f_P) = l[P] - l[Q]$ than the *Tate pairing* is $\tau(P,Q) = \frac{f_P(Q+S)}{f_P(S)}$ and the *modified Tate pairing* is $\hat{\tau}(P,Q) = \tau(P,Q)^{\frac{q-1}{l}}$.

Definition: Let E be an elliptic curve over $F_p, m \geq 1, p \nmid m$, the *embedding degree* of E with respect to m is the smallest positive k such that $E(F_{p^k})[m] = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

Theorem: Let E be an elliptic curve over $F_p, p \nmid m$ and suppose E has an element of prime order $l \neq p$. The embedding degree, k is one of the following: (1) $k = 1$ $(l \leq \sqrt{p} + 1)$; (2) $k = l$ if $p = 1 \pmod{l}$; (3) if $p \neq 1 \pmod{l}$, k is the smallest positive integer such that $E(F_{p^k}) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

MOV Algorithm: Under the same conditions as the theorem:

1. Compute $N = \#E(F_{p^k})$, $l \mid N$;
2. Choose, at random, $T : T \in E(F_{p^k}), T \notin E(F_p)$;
3. Compute $T' = (N/l)T$. If $T' = O$, repeat step 2.
4. $lT' = O$, compute $\alpha = e_m(P, T')$ and $\beta = e_m(Q, T')$;
5. Solve $\beta = \alpha^n$ in $E(F_{p^k})$;
6. $Q = nP$.

Definition: Let $l \geq 3$, $P \in E[l]$, $lP = O$, $\psi : E \to E$. ψ is a *distortion map* for P if (a) $\psi(nP) = n\psi(P)$ and (b) $e_l(P, \psi(P))$ is a primitive l-th root of unity.

Theorem: If $E[l] = \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$, TFAE: (a) P, Q is a basis for $E[l]$; (b) $p \neq O$ and there is no $\alpha : Q = \alpha P$;

(c) $e_l(P,Q)$ is a primitive l-th root of unity.

Note: the *decision ECDLP problem* is in $NP \cap co-NP$. Attacks (1) Exhaustive Search - to avoid, make sure $\#E_q = nh$, n a large prime $> 2^{160}$, h, small; (2) Pohlig-Hellman/Pollard-ρ use Pohlig to reduce from $n = p_1^{e_1}...p_t^{e_t}$ to p, since this step is easy, want p large, Pollard costs $O(\sqrt{p})$ [For Pollard, "random" function is $f(X) = X + a_j P + b_j Q \pmod p$.]; (3) Isomorphism attack; (4) MOV for anomalous curves - to avoid make sure $q = p^m$ and $p \nmid \#E_q$; (5) Weil-Tate pairing - to avoid make sure $n \nmid (q^k - 1), k \leq C$ and that the DLP problem for F_{q^C} is intractable; (6) Weil descent - to avoid, if $q = 2^m$, make sure m is prime. Index calculus attack is unlikely because the lifting required from $E_q(a,b)$ to $E_{\mathbb{Q}}(\overline{a},\overline{b})$ is unknown and the number of points of small height in elliptic curves over $\mathbb{Q}$ is small.

Lenstra Elliptic Curve Factoring Method:

1. $(n,6) = 1, n \neq m^r$.
2. Choose random b, x_1, y_1 between 1 and n.
3. $c = {y_1}^2 + {x_1}^3 - bx_1 \pmod n$.
4. $(n, 4b^3 + 27c^2) = 1$.
5. $k = lcm(1,2,\ldots,K)$.
6. Compute $KP = (\frac{a_k}{{d_k}^2}, \frac{b_k}{{d_k}^3})$
7. $D = (d_k, n)$ If $D = 1$, go to 5 and bump K or go to 2 and select new curve.

1.5.3 Elliptic, Weierstrauss and Fermat

Definition: Two curves C, D are projectively equivalent if there is a projective transformation ϕ with $\phi(C) = D$. Every nonsingular cubic is equivalent to a curve which in affine coordinates is $y^2 = 4x^3 - g_2 x - g_3 = 0$. This is the *Weierstauss normal form.* Note: To prove show that every non-singular curve has an inflexion point (triple tangent). Map flex to $(0,0,1)$.

Elliptic Functions from Trigonometry: $S(x) = \int \frac{dx}{\sqrt{1-x^2}}$. Let $\frac{dx}{du} = c(u)$, $s(u)^2 + c(u)^2 = 1$. $s'(u) = c(u)$, $c'(u) = -S(u)$, $s(-u) = -s(u)$ and $c(-u) = c(u)$. $s(x+y) = s(x)c(y) + s(y)c(x)$ and $c(x+y) = c(x)c(y) - s(y)s(x)$. $\Omega : R \to S^1$ (S^1 is the 1-sphere - circle) by $u \mapsto (c(u), s(u))$ is a morphism: $\Omega(x+y) = \Omega(x) \oplus \Omega(y)$. Ω has a non-trivial kernel K since S^1 is compact but R isn't. $K = 2\pi\mathbb{Z}$. These functions are periodic, satisfy the given derivatives, parameterize S^1 under the indicated morphism and provide the integration property. By analogy, set $F(k,v) = \int \frac{dz}{\sqrt{(1-z^2)(1-k^2z^2)}}$ and define sn by $F(k, sn(u)) = u$. $cn(u) = \sqrt{1 - sn^2(u)}$, $dn(u) = \sqrt{1 - k^2 sn^2(u)}$. sn, cn, dn are doubly periodic with periods ω_1, ω_2.

Weierstrauss Parameterization: $y(t)^2 = x(t)^3 + ax(t) + b$. Let $\omega_1, \omega_2 \in \mathbb{C}$ and $\Lambda = \{a\omega_1 + b\omega_2 : a, b \in \mathbb{Z}\}$ which is preserved under unimodular transformations, $\Lambda' = \lambda - \{\vec{0}\}$. $\mathbb{C}/\Lambda$ is an equivalence class of complex numbers equivalent to a torus.

Theorem: Any two basis of the same discrete group of an elliptic (doubly periodic) function are related by *unimodular* transformations. The period module of a doubly periodic function is one of the following: (1) 0; (2) $n\omega, n \in \mathbb{Z}$; (3) $n\omega_1 + m\omega_2, n, m \in \mathbb{Z}$. In the latter case, there is a canonical basis (ω_1, ω_2) with $\tau = \frac{\omega_2}{\omega_1}$ such that (i) $Im(\tau) > 0$, (ii) $-\frac{1}{2} \leq Re(\tau) \leq \frac{1}{2}$, (iii) $|\tau| \geq 1$ and $Re(\tau) > 0$ if $|\tau| = 1$.

Proof: Suppose neither (1) or (2) hold. Let ω_1 be the element of M with smallest non zero modulus and let ω_2 be the element of $M \notin \{m\omega_1\}$ with the smallest non-zero modulus. First, if $\frac{\omega_2}{\omega_1} \in \mathbb{R}, \exists n : n < \frac{\omega_2}{\omega_1} < n+1$ which means $|n\omega_2 - \omega_1| < |\omega_1|$ which is a contradiction. We may put $\omega = \lambda_1\omega_1 + \lambda_2\omega_2, \lambda_1, \lambda_2 \in \mathbb{R}$ so $\exists m_1, m_2 \in \mathbb{Z} : |\lambda_1 - m_1| \leq \frac{1}{2}, |\lambda_2 - m_2| \leq \frac{1}{2}$. But then $\omega' = \omega - m_1\omega_1 - m_2\omega_2 \in M$ and $|\omega'| \leq \frac{1}{2}|\omega_1| + \frac{1}{2}|\omega_2| \leq |\omega_2|$. To show (i, (ii), (iii) and (iv), pick ω_1 and ω_2 as above. We already have, $|\omega_1| \leq |\omega_2|$, $|\omega_2| \leq |\omega_1 + \omega_2|$, $|\omega_2| \leq |\omega_1 - \omega_2|$. If $Im(\tau) < 0$ replace (ω_1, ω_2) with $(-\omega_1, \omega_2)$. If $Re(\tau) = -\frac{1}{2}$ replace (ω_1, ω_2) with $(\omega_1, \omega_1 + \omega_2)$. If $|\tau| = 1$ and $Re(\tau) < 0$ replace (ω_1, ω_2) with $(-\omega_2, \omega_1)$.

Theorem: An elliptic function without poles is constant.

Theorem: If f is elliptic, $\sum_{a \in \mathcal{P}} Res(f, a) = 0$, $\mathcal{P}$ is the set of *poles*.

Theorem: If f is elliptic, M is the module of periods, $\langle a_1, \ldots, a_n \rangle$ are the zeros, $\langle b_1, \ldots, b_n \rangle$ are the poles then $\sum_i a_i = \sum_i b_i \pmod{M}$.

Elliptic functions of order 2: $\wp(z) = z^{-2} + a_2x^2 + a_4z^4 + \ldots$. $\wp(z) = \frac{1}{z^2} + \sum_{\omega \neq 0} \frac{1}{(z-\omega)^2)} - \frac{1}{\omega)^2}$. If $|\omega| \geq 2|z|$, $|\frac{1}{(z-\omega)^2)} - \frac{1}{\omega)^2}| \leq \frac{10|z|}{|\omega|^3}$. $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp - g_3 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$, e_1, e_2, e_3 are distinct. The equation can be solved by $z = \int^w \frac{dw}{\sqrt{4w^3 - g_2w - g_3}}$. Since $\wp(\omega_1 - z) = \wp(z)$, $\wp'(\frac{\omega_1}{2}) = 0$; similarly, $\wp'(\frac{\omega_2}{2}) = 0$ and $\wp'(\frac{\omega_1+\omega_2}{2}) = 0$. So $e_1 = \frac{\omega_1}{2}$, $e_2 = \frac{\omega_2}{2}$, and $e_3 = \frac{\omega_1+\omega_2}{2}$. Put $\lambda(\tau) = \frac{e_3 - e_2}{e_1 - e_2}$. λ is the quotient of two analytic functions in the upper half-plane.

Definitions: If $\lambda(\frac{a\tau+b}{c\tau+d}) = \lambda(\tau)$, the linear transformation is an *automorphism* of $\wp$. The automorphisms $\lambda(\frac{a\tau+b}{c\tau+d}) = \lambda(\tau)$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2$ form the *modular group*. $\lambda(\tau + 1) = \frac{\lambda(\tau)}{\lambda(\tau)-1}$, $\lambda(\frac{1}{\tau}) = 1 - \lambda(\tau)$. $\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda'}(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2})$.

Theorem: $\wp(z, \Lambda)$ converges uniformly for $\mathbb{C}/\Lambda$, $\wp(z) = \wp(-z)$ and $\wp$ is doubly periodic. As z ranges over a fundamental region, $\wp$ takes on every complex value twice. $\wp(z, \Lambda) - \frac{1}{z^2} = \sum_{\omega \in \Lambda'}(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}) = \sum_{n=1}^{\infty}(n+1)z^n(\sum_{\omega \in \Lambda'} |\frac{1}{\omega^{n+2}}|)$. The final summation is an Eisenstein series of weight $n+2$, denoted G_{n+2}. $\wp(z) = \frac{1}{z^2} + 3G_4z^2 + 5G_6z^4 + \ldots$. $P(z) = (\wp'(z), \wp(z))$ is a point on $y^2 = 4x^3 - 60G_4x - 140G_6$.

Reimann surfaces: Glue two copies of C to get $\sqrt{z}$. For $N \in \mathbb{Z}, N > 0$ define $\Gamma_0(N) \subseteq SL_2$ with $N|c$. $\Gamma_0(N)$ acts on H and $H/\Gamma_0(N) \equiv X_0(N)\backslash K$ where K are the cusps. $X_0(N)$ is compact and the members are the modular functions of level N.

Semi-Stable: For all primes $l > 3$, $l|Disc$ and only two of the roots are equal $\pmod l$. Frey curve: $C_{a,b}^F \stackrel{\text{def}}{=} y^2 = x(x - a^p)(x - b^p)$. If b is even and $a = -1 \pmod 4$. Frey curve is semi-stable.

Definitions: Denote $E_{A,B,C,D}(\mathbb{Q}) \stackrel{\text{def}}{=} y^2 = Ax^3 + Bx^2 + CX + D, A, B, C, D \in \mathbb{Q}$. Define b_p to be the number of solutions to $E_{A,B,C,D}(\mathbb{Q}) = 0$. E is *modular* if $\exists$ eigenfunction, $f(z) = \sum_n a_n e^{2\pi i n z}$. $E/\mathbb{Q}$ is

modular if $\exists f$ and eigenfunction with $a_p = p + 1 - b_p$ for all but finitely many p.

Taniyama-Shimura Conjecture: Every elliptic curve is modular. Alternate T-S: $E(A, B, C, D)$. $\exists$ modular functions $f(z), g(z)$ such that $g(z)^2 = Af(z)^3 + Bf(z)^2 + Cf(z) + D$.

Define the *conductor* $Cond_{a,b,c} = \prod_{p|abc} p$. Two elliptic curves are isomorphic iff their *j-invariants* are equal. The j-invariant of $C^F_{a,b} = 2^8 \frac{(a^{2p}+b^{2p}+a^p b^p)^3}{a^{2p}b^{2p}c^{2p}}$. If $F(\frac{az+b}{cz+d}) = (cz+d)^2 F(z)$, F is a modular form of weight 2.

Proof of Fermat's Last Theorem: Suppose it's false and that $a^p + b^p = c^p$ is a counterexample. Let $C^F_{a,b}$ be the Frey curve. $Disc(C^F_{a,b}) = a^{2p}b^{2p}c^{2p}$ so $C^F_{a,b}$ is semi-stable. Wiles proved every semi-stable elliptic curve is modular so $C^F_{a,b}$ is modular and has a cusp form of weight 2 and level N where N is the conductor. If l is an odd prime and $l|N$, by Serre, we can obtain a new F of weight 2 of level N/l. By induction, keep doing this until $N = 2$. The dimension of the space of cusps is equal to the genus of compact Reimann surface $X_0(N)$. But $Genus(X_0(2)) = 0$, so there is no such cusp forms of weight 2, level 2. This contradiction establishes the theorem. Incidentially, the restriction of semi-stability in Wiles Theorem has been removed.

Chapter 2

Computer Science

2.1 Basics

Definitions: $f \in O(g) \leftrightarrow g \in \Omega(f) \leftrightarrow L_{x\to\infty}\frac{f(x)}{g(x)} < \infty$. $f \in o(g) \leftrightarrow g \in \omega(f) \leftrightarrow L_{x\to\infty}\frac{f(x)}{g(x)} = 0$. $G_1 \subset (G, E)$ is a *strongly connected component* iff $x, y \in G_1$ means there is a directed path $x \to y$ and a directed path $y \to x$.

Recurrences: Suppose $T(n) = aT(n/b) + f(n)$. If $f(n) = O(n^{log_b(a)-\epsilon})$ then $T(n) = \Theta(n^{log_b(a)})$. If $f(n) = \Theta(n^{log_b(a)})$ then $T(n) = \Theta(n^{log_b(a)}lg(n))$. If $f(n) = \Omega(n^{log_b(a)+\epsilon})$ and $af(n/b) \leq cf(n), c < 1$ then $T(n) = \Theta(f(n))$.

Binary arithmetic: Adding an m bit number and n bit number takes $O(max(m, n))$ time and $O(m + n)$ space. Multiplying an m bit number and n bit number takes $O(mn)$ time and $O(m+n)$ space. The *extended gcd* of an m bit number and n bit number takes $O(mn)$ time and $O(m + n)$ space. $GCD(u, v)$ average running time: $O((1 + \frac{max(u,v)}{(u,v)})lg(min(u, v)))$. $A^E \pmod M$ where M is an m bit number and E is an n bit number takes $O(nm^2)$ time.

Theorem: Given $\epsilon > 0$ there is a multiplication algorithm such that the number of elementary operation $T(n)$ needed to multiply two n-bit numbers satisfies $T(n) < c(\epsilon)n^{1+\epsilon}$. Strassen: $T(n) = O(nlg(n))$.

Floating Point Numbers: $f \times b^{e-q}$ is represented as (e, f).

Heapsort: For a node, t, the *heap property* is $value(t) \geq value(LEFT(t))$ and $value(t) \geq value(RIGHT(t))$. A heap list $A[1], A[2], \ldots, A[n]$ can represent a heap with $LEFT(A[i]) = A[2i]$ and $RIGHT(A[i]) = A[2i+1]$. Note that a path from a node to an edge is linearly ordered and so largest element is at root. Usually the heap is arranged so that $value(LEFT(t)) \geq value(RIGHT(t))$.

```
heapify(A,i,j,n)
{
    if(i is not a leaf) {
        k= child of i with largest elment;
        if(A[k]>A[i]) {
            swap (A[i], A[k]);
            heapify (A, k, j, n);
        }
    }
}

buildheap(A,n)
{
```

```
    for(i=n;i>1;i--) {
        heapify(A,i,n,n);
    }
}

heapsort(A,n)
{
    buildheap(A,n);
    for(i=n;i>1;i--) {
        swap(A[1], A[i]);
        heapify(&A[1],i-1, i-1);
    }
}
```

Shortest Path: between x and y in $G = (V, E)$ where $l(e) > 0$ the weight of $e \in E$ is $O(elg(n))$. d(v) contains an overestimate of the shortest path from s to v. $prev(v)$ contains the previous element in the shortest path from s to v. (Ford-Bellman version works for negative weights.)

```
shortestpath(V,E,s)  {
    for (v in V) {
        d(v):= infinity;
        prev(v):= empty-set;
        }
    H:= empty-set;
    d(s)= 0;
    mark(s);
    while (H is not empty) {
        h= deletemin(H);
        for e=(v, w) in E, w unmarked) {
            if(d(w)>(d(v)+l(e))) {
                d(w)=d(v)+l(e);
                prev(w)= v;
                insert(w, H);
                }
            }
        }
    }
```

Union-find: Link(x, y): make x and y kids of a common parent. Parent node points to itself. m UNION-FIND operations on n elements is $O((m + n)lg(n))$.

```
makeset(x) {
    p(x)= x;
    rank(x)= 0;
    }

find(x) {
    if(x != p(x))
        p(x)=  find(p(x));
   return(p(x));
   }
```

```
link(x, y) {
    if(rank(x)>rank(y)) swap(x, y);
    if(rank(x)==rank(y)) rank(y)++;
    p(x)= y;
    return(y);
    }

union(x,y) {
    link(find(x), find(y));
    }
```

Order statistics: The algorithm below satisfies the recurrence $T(n) \leq T(\frac{n}{5}) + T(\frac{3n}{4} + cn)$.

Select(k,S)
{
  if($k < 50$) sort and return k'th element;
  Partition S into 5 sequences $S_1, \ldots, S_{\lfloor \frac{|S|}{5} \rfloor}$, T, where T contains the up to 4 leftovers;
  Sort each 5 set;
  Let M be the set of the medians for the S_i;
  m= Select($\lceil \frac{|M|}{2} \rceil$;
  let S_1, S_2, S_3 be the sets of elements $<, =, > m$ respectively;

if($|S_2| > k$)
return Select(k, S_1);
if($|S_1| + |S_2| > k$)
return m;
return($k - |S_1| - |S_2|$, S_3);
}

$2-3$ **Trees:** Interior node has smallest key of 2nd and 3rd descendant. Insert: Do membership test stop at terminal position; id 2 kids, add one, if not, split into two, (n, n'). Add n' using insert. Delete: If two kids left, done. Otherwise, try to move node of a siblings under common parent; if you can't, transfer this node to a sibling. If this leaves a singleton, in the parent, recurse the transfer on parent.

Minimal spanning trees: Consider a graph, $G = (V, E)$, each edge $e \in E$ having weight $wt(e)$.
Kruskal:
Initialize a forest of trees consisting of V.
while(there is more than one component)
1. Remove edge from E of minimum weight.
2. Add it if it unites two trees. Discard it if it creates a cycle.

Prim:
1. Choose an arbitrary vertex $S = \{x\}$, $M = \emptyset$.
2. while($S \neq V$)
3. Choose an edge $e = (x, y), x \in S$ of minimum weight.
4. If $y \in S$, discard. Otherwise $M = m \cup \{e\}$

NP Completeness: $P \subseteq N$. If $A \leq B$ [1] and $B \in P$ then $A \in P$. $L \in NPC$ if and only if $L \in NP$, $A \in NP \rightarrow A \leq L$. Classical computation theory classifies problems by a "certain" solution on all instances. The class of problems which can be solved in polynomial time "up to an arbitrary error, ϵ" is called RP for "randomized polynomial." $P \subseteq RP \subseteq NP$.

Problems in P and NP: P: MST. Given a weighted graph, G, and a weight, K $\exists$ a tree, NP: TSP. Given a weighted graph, G, and a weight, K $\exists$ a cycle, C, that connects all nodes of G with weight $\leq K$.
P: Circuit value. NP: Circuit SAT.
P: 2-SAT: Use $\phi = (a_1 \vee b_1) \wedge ... \wedge (a_n \vee b_n)$ to form graph with nodes $a_i, b_i, \overline{a_i}, \overline{b_i}$ insert edges $\overline{a_i} \rightarrow b_i$ and $\overline{b_i} \rightarrow a_i$. Find strongly connected components. If no strongly connected component contains a variable and its negation, it is satisfiable; otherwise not. So 2-SAT is not NP hard. NP: 3-SAT. Note in disjunctive normal form SAT is easy but translating is hard.
P: matching. NP: 3D matching.
P: Linear Programming. NP: Integer Programming.

Ford-Fulkerson: Augmenting path p is a simple path from s to t that increases the flow.

```
Initialize flow, f to 0;
while (there is an augmenting path, p)
    augment flow along p;
return f;
```

Undecidability: Suppose $Term(P, X)$ is a boolean function which takes a program, P, and an input X.

[1] $A \leq B$ means problem A can be transformed to problem B in polynomial time; this is called a reduction *from A to B*.

$Term(P, X)$ returns true iff P terminates on X. $Term(P, X)$ returns false iff P does not terminate on X.

Theorem: $Term(P, X)$ does not exist. Suppose it did. Set

```
diag(P,X) {
  if $Term(P,P)$==true
    loop
    }
```

$diag(diag)$ terminates iff it doesn't terminate. Contradiction.

Stable Matching (up to n^2 rounds). (1) Boy goes to favorite girl on list. (2) Girl tells highest choice "maybe", tells everyone else No. (3) Boy crosses off girls that have said no. (4) terminate in the round when every girl has told one boy "maybe", convert "maybe" to yes.

Linear Programming Standard Form: Maximize $x = C^T X$, subject to $AX = B$, $X \geq 0$. Problem: There may be exponentially many corners. (Reason: introduce to n constraint inequalities m slack variables; the corner points occur when m variables are 0. There are $\binom{m+n}{m}$ ways to select the variables to be set to 0.) Simplex idea: move along growing paths instead of trying all corners randomly. Dual, minimize $x = B^T W$, subject to $A^T W = C$, $W \geq 0$.

Notation: *basic variables* $\neq 0$, *non basic variables* $= 0$. A is an $m \times n$ matrix, with m variables (including slack) and m constraints. Tableau has basic variables and their values in two first columns. Top row is all variables as labels middle is matrix (A). Rightmost column is constants (B). Bottom row is $C - C^T X$ in terms of the non-basic variables. Basic algorithm is:

1. Locate most negative coefficient in bottom row, call column containing it x_j.
2. Compute $\frac{B_i}{A_{ij}}$. The smallest one, denoted k, is the pivot.
3. Convert pivot to 1 and eliminate all coefficients in the same column.
4. Replace x_k row by x_j.
5. repeat until no negative numbers in bottom row.

SAT/k-sat reduction: $l_1 \vee l_2 \vee \ldots \vee l_n \rightarrow l_1 \vee l_2 \vee x_1 \wedge \overline{x_1} \vee l_3 \vee x_2 \wedge \ldots \overline{x_{n-3}} \vee l_{n-1} \vee \ldots \vee l_n$. Phase transition for SAT: $\frac{clauses}{variables} \approx 4.3$. 3-SAT $\rightarrow$ MQ. Replace + with $\vee$, $\cdot$ with $\wedge$, 1 with true, 0 with false. If $c_i = x_{i_1} \vee x_{i_2} \vee x_{i_3}$ add $x_{i_1} + x_{i_2} + x_{i_3} x_{i_4}$ and $x_{i_1} \cdot x_{i_2} + x_{i_2} \cdot x_{i_3} + x_{i_1} \cdot x_{i_3} = x_{i_5}$ and $x_{i_4} + x_{i_5} + x_{i_4} \cdot x_{i_5} = 1$.

Theorem: The following problems are NP Complete: SAT, k-SAT ($k > 2$), k-clique, Vertex Cover, Independent set, Subset Sum, Partition, Bin Packing, Hamilton circuit. *Clique/SAT reduction:* Each occurrence of a variable is a vertex, edges between vertices if their occurrence in the clauses have same complementarity. k is number of clauses.

Hard core bit: Let f be a one-way function from $\{0,1\}^n$ to $\{0,1\}^n$, $x \in \{0,1\}^n$, $r \in \{0,1\}^n$, and let G be a function that takes $\{0,1\}^n$ to $\{0,1\}^{n+1}$ by $G(x,r) = f(x), r, < x, r >$. Let P be a prediction function. Goldreich-Levin: If there is an algorithm A such that $|Prob_r[A(f(x), r) =< x, r >] - \frac{1}{2}| \geq \epsilon$ then there is an algorithm I that produces a list L of size $\leq \frac{1}{\epsilon^2}$ with x in L, (2) I runs in time polynomial in n and $\frac{1}{\epsilon}$ and doesn't compute f. A function is *negligible:* smaller that inverse of any polynomial. Witness: $w : \Sigma^* \rightarrow P(\Gamma^*)$. *Decision problem:* $A_w \subseteq \Sigma^*$, $A_w = \{x \in \Sigma * | w(x) \neq 0\}$. *Example:* $x \in \Sigma^*$ is an encoding

of a Boolean Form. $y \in \Gamma*$ is an encoding of a truth assignment. $\#P$ is class of witnesses, w, such that: (i) there is a P-time algorithm to decide if $x \in w(x)$ and (ii) $\exists k \in N$ such that $\forall y \in w(x), |y| \leq |x|^k$. $w \in \#P \rightarrow A_w \in NP$ and $A \in NP \rightarrow \exists w, A = A_w$.

Theorem: Counting perfect matchings of a bipartite graph is $\#P$ complete.

Finite State Machine: Finite alphabet, A, finite states, S, two functions: $\delta : S \times A \rightarrow S$ and $\gamma : S \times A \rightarrow A$. Finite State Automata is FSM without output.

Regular expressions: Language L is a subset of A^*. *Regular expression*, R over alphabet, A with letters $a \in A$: (1) $\epsilon \in R$, (2) $a \in A$, (3) $r^* \in R$ if $r \in T$, (4) $r_1 r_2 \in R$ if $r_1, r_2 \in R$, (4) $r_1 \vee r_2 \in R$ if $r_1, r_2 \in R$. Language associated with a regular expression: (1) $L(\epsilon) = \{\epsilon\}$, (2) $L(a) = \{a\}$, (3) $L(r^*)L(r)^*$, (3) $L(r_1 r_2) = L(r_1)L(r_2)$, (4) $L(r_1 \vee r_2) = L(r_1) \cup L(r_2)$. L is a *regular language* if $\exists r \in R$ with $L = L(r)$. *Phrase structured Grammar*, G, consists of (1) Vocabulary V, (2) terminals (denoted by lower case letters) $T \subseteq V$, (3) variables or non-terminals $V \setminus T$ (denoted by upper case letters), (4) a designated non-terminal S, called the start symbol, (5) a finite set P of productions: $\alpha \rightarrow \beta$. $w \Rightarrow w'$ iff $\exists u, v, w = u\alpha v$ and $w' = u\beta v$.

Grammars: Grammar types are defined by production rule limitation: (1) Type 0: no limitations, (2) Type 1: production rules of the form $\alpha \rightarrow \beta$, $|\alpha| \leq |\beta|$ or $\alpha \rightarrow \epsilon$, (3) Type 2: production rules of the form $A \rightarrow \beta$, (4) Type 3: production rules of the form $A \rightarrow a$ or $A \rightarrow aB$, (5) *context free:* production rules of the form $A \rightarrow \beta$, (6) *context sensitive:* production rules of the form $\alpha A \alpha' \rightarrow \alpha\beta\alpha'$, (7) regular: production rules of the form $A \rightarrow a$, $A \rightarrow aB$ or $S \rightarrow \epsilon$. Backus-Naur form for type 2 context free grammar: (i) ::= replaces $\rightarrow$, (ii) non-terminals enclosed in brackets <> and (iii) all productions with the same non-terminal LHS are combined into a single RHS. *Example:* $\langle sentence \rangle$ ::= $\langle noun\ phrase \rangle \langle verb\ phrase \rangle$, $\langle noun\ phrase \rangle$ ::= $\langle noun \rangle | \langle article \rangle \langle noun \rangle$, $\langle noun \rangle$::= boy.

Theorem: A language L can be generated by a type 3 (regular) grammar iff there is a finite automaton M that accepts L. Pushdown automata (with infinite stack) recognize L iff L is context free. L is recognized by a linear bounded automata (tape linearly bounded in length of input) iff L is context sensitive.

Minimizing state machines: Two states, s_i, s_j, are 0 equivalent if the states have the same output for every input. States are $k+1$ equivalent if they have the same outputs for any input and their successor states are k equivalent. Minimization procedure: Define π_0 as all states that are 0 equivalent. Do until no further refinement happens: sub-partition π_k into π_{k+1} into subblocks are $k+1$ equivalent. This terminates. When it does, merge equivalent states.

Pumping Lemma: Let L be a finite state grammar accepted by a finite state machine, M, with n states. If α is a string accepted by M of length at least n, then $\alpha = u||v||w$ where $u||v^i||w$ is also in L.

Definition: Turing machines are FSMs with a bi-directionally infinite tape with a finite number of premarked squares and an additional transition function $\sigma : S \times A \rightarrow \{L, R, HALT\}$.

Huffman algorithm: Label each node with frequency. As long as more than one node is present, take the two nodes with the lowest frequency and combine them into a single node with the two combinants as children. New node has combined frequency. Left subnode has lower of two frequencies, right the higher. Read code by traversing from root. Left traversal at parent is 0, right, 1.
Resulting code is prefix free. Further $H(X) \leq l(x) \leq H(X) + 1$.

2.1.1 Concurrency

```
ECMA Consistency
    1. Reads and writes cannot move before volatile read.
    2. Reads and writes cannot move after volatile write.

CompareExchange(ref int loc, int value, int comp) {
    Monitor.Enter;
    ret= loc;
    if(ret==comp) loc= value;
    Monitor.Exit;
    return ret;
}

class SpinLock {
    volatile int isEntered=0;   // 1 if lock acquired
    int Enter() {
        while(CompareExchange(isEntered,1,0)!=0);
        }
    Exit() {
        isEntered= 0;
    }
}

Memory Consistency Rules
    1. Behavior of Thread in isolation is unaffected
    2. Reads cannot move before lock
    3. Writes cannot move after lock
```

```
DPLL(C,A) {
// C: clauses, A: literal assignments
//      Termination:
//              empty clause: unsatisfiable
//              empty set of clauses: satisfiable
    if(A is empty)
        return SATISFIED;
    if(A has an empty clause)
        return UNSATISFIABLE;
// unit clause is a clause with one literal
    if unit clause (l) occurs in A
        return DPLL (assign(l,C), A + l));
    if l occurs with same polarity throughout
        return DPLL (assign(l,C), A + l));
    l= choose-literal(A);
        return DPLL (assign(l,C), A + l)) OR
               DPLL (assign(not l,C), A + not l));
        }
Note: If A, B, C are p-free,
(A | p) & (B|!p) &C) is inconsistent iff (A|B)&C is.
Chase(C,x) {
    set x to t;
    delete all clauses containing x from C;
    delete all occurences of !x from clauses in C;
    if (empty clause)
        return UNSATISFIABLE;
    if (unit clause l)
        return Chase(l,t);
    if (C is empty)
        return SATISFIED;
```

```
Priority Queue (arrays start at 1 here)
```

```
ExtractMax(A) {
    if(heapsize(A)<1)
        return error;
    max= A[1];
    A[1]= A[heapsize(A)];
    heapsize(A)=heapsize(A)-1;
    Heapify(A,1);
    return max;
}
```

```
Insert(A,k) {
    heapsize(A)=heapsize(A)+1;
    i= heapsize(A);
    while(i>1 & A[parent(i)]<k) {
        A[i]= A[parent(i)];
        i= parent(i);
        }
    A[i]= k;
    }
```

```
Select(A,k) {
    // select kth element from A[1,...n-1]
    if(k==0) return min(A);
    // For randomized, choose x in A at random
    x= SideSelect(A);
    Set B= < y in A: y <=x>
    Set C= < y: y>x >
    if(k<|B|) return Select(B,k)
    return Select(C,|B|-k);
    }
```

```
SideSelect(A,k) {
    for(i<=0<=n=INT(size(A)/5))
        Sort successive 5 elements
        // A[5i]<=A[5i+1]<=A[5i+2]<=A[5i+3]<=A[5i+4]
    R= < A[5i+2] > , 0<=i<=n
    x= SideSelect(R,Size(R)/2);
    // note x <= 3*INT((n-5)/10) elements.
    }
// Note E(T(n))= E(T(sn))+n,  x ~ 3/4
```

```
struct semaphore {
    int count;
    ProcessQueue queue;
    };
```

```
void V(semaphore s) {
    if(s.queue.empty())
        (s.count)++;
    else
        s.queue.remove(); //schedule process
    }
```

```
void P(semaphore s) {
    if(s.count>0) {
         (s.count)--;
    else
         s.queue.Insert(); // block
    }
```

```
shared semaphore s= 1;
     P(s);
     //critical section
     V(s);
```

```
Map()
Reduce()
Scan()      // || prefix
Scatter()
Gather()
```

```
Readers/writers
linear sweep
```

Architecture and current PCs: $P = C \times V^2 \times f$. *Big endian* word: $0, 1, 2, 3$ (descending byte address). *Little endian* word: $3, 2, 1, 0$ (descending byte address).

Optimization Level	Description	Level
High	Procedure inlining	3
Local	common subexpression	1
Local	constant propagation	1
Local	stack height reduction (expression tree)	1
Global	global common subexpression	2
Global	global constant propagation	2
Global	code motion	2
Global	induction variable elimination	2
Global	loop unrolling	4
Global	strip mining	4
Arch specific	strength reduction	1
Arch specific	pipeline scheduling	1
Arch specific	branch offset	1

Effect on performance of Bubblesort (100K items). Base is 300MHz Sparc Ultra.

Optimization level	Relative performance	Clocks	Instructions	CPI
0	1.00	158,615	114,938	1.38
1	2.37	66,990	37,470	1.79
2	2.38	66,521	39,993	1.66
3	2.41	65,747	44,993	1.46

SRAM: $.5 - 1ns$, $4,000\$/GB$. DRAM: $50 - 70ns$, $100\$/GB$. Disk: $10^7 ns$, $1\$/GB$. Dram address setup: 1 memory cycle, access time: 15 cycles, data transfer: 1 cycle. 4-way interleave plus multiword block gets time down to 20 cycles on average. Miss penalty to main: 500 cycles, to L2: 25 cycles. TLB: 512 entries. Miss: 100 cycles. Miss percentage; .5-1. Disk seek latency: 10 ms, rotational latency: 5 ms, transfer rate: 50 MB/s, MTTF: 10^6 hours. Bus speed: system (800 MHz), NB (266 MHz), SB (33 MHz). Bandwidth:

Device	Bandwidth
Memory	3.2GB/sec
Disk	150 MB/sec
AGP	2.1 GB/sec
PCI	132 MB/sec
NIC	20 MB/sec

Dwarves: Finite state machines, combinatorics, graphs, Structured/unstructured grids, dense matrix, sparse matrix, map-reduce, backtrack/branch-and-bound, N-body, FFT, Graphical models.

***LU*-factorization:** Let $A \neq 0$ be an $m \times n$ matrix. There are permutation matrices P, Q such that $P^T AQ = LU$ where L is lower triangular and U is upper triangular. QR-factorization: Let $X \in \mathbb{C}^{n \times p}$ have rant p then $x = QR$ where Q is an orthogonal matrix and R is an upper triangular matrix. QR-factorization via unitary operations is used in the least square approximation problem. Spectral decomposition: $U^H AU = diag(\lambda_1, \lambda_2, \ldots, \lambda_n)$. The eigenvalues of $X^H X$ are the sequence of singular values of X. For a $p \times q$ matrix, row major storage is $A[1,1] = a[1]$, $A[1,2] = a[2]$, $\ldots$, $A[2,1] = a[q+1]$, etc., and in general, row major storage is $A[i,j] = a[(i-1)q + j]$, column major storage is $A[1,1] = a[1]$, $A[1,2] = a[q+1]$, $\ldots$, $A[2,1] = a[2]$, etc., and in general, column major storage is $A[i,j] = a[(j-1)p + i]$. One step of Gaussian Elimination:

$$\begin{pmatrix} \alpha_{11} & \alpha_{12}^T \\ \alpha_{21} & A22 \end{pmatrix} = \begin{pmatrix} \beta_1 \\ b_2 \end{pmatrix} \rightarrow \begin{pmatrix} \alpha_{11} & \alpha_{12}^T \\ 0 & A22 - \alpha_{11}^{-1}\alpha_{21}\alpha_{12}^T \end{pmatrix} = \begin{pmatrix} \beta_1 \\ b_2 - \alpha_{11}^{-1}\beta_1\alpha_{21} \end{pmatrix}$$

Definition: A *hard core predicate* of a one-way function, f is easy to compute given x but not given $f(x)$. If f is a one-way function, $g(x,r) = (f(x),r)$ is a hard core predicate. Let $B_x(y) : \{0,1\}^n \rightarrow \{0,1\}$ be a probabilistic oracle with ϵ advantage for (x,y), that is, $Pr(B_x(y) = (x,y)) = \frac{1+\epsilon}{2}$ and let $EQ_x(y)$ be an oracle for $x = y$. Define $Gd_B = \{y : B_x(y) = (x,y)\}$ and $Bd_B = \{y : B_x(y) \neq (x,y)\}$ so $|Gd_B| = \frac{1+\epsilon}{2}2^n$ and $|Bd_B| = \frac{1-\epsilon}{2}2^n$.

Goldreich-Levin: Let $R = \langle r_1, \ldots, r_m \rangle$ be a random selection of elements from $[n]$, $z \in [n]$ and $b_j = (x, r_j)$. Let $\langle S_j \rangle$ be a fixed enumeration of the subsets of $[m]$. $R[S] = \sum_{j \in S} r_j$. Define the following algorithm:

$STRONG - SC^{B_x}(z, r_1, \ldots, r_m, b_1, \ldots, b_m)$
  $sum = 0$;
  for$(i = 1; i \leq 2^m))$ {
    $R(S_i) = \sum_{j \in S_i} r_j$;
    $B[S_i] = \sum_{j \in S_i} b_j$;
    $c = B_x(z + R[S_i]) - b[S_i]$;
    $sum+ = c$;
    }
  return $sum > \frac{2^m}{2}$;

Define the following algorithm:

$RECOVER^{B_x, EQ_x}(1^n)$
  Pick $r_1, \ldots r_m \in [n]$ at random;
  for$(i = 1; i \leq 2^m))$ {
    $(b_1, \ldots, b_m)_2 = i - 2$;
    for$(k = 1; k \leq n)$
      $y^{(k)} = STRONG - SC^{B_x}(e_k, r_1, \ldots, r_m, b_1, \ldots, b_m)$;
    $y = y^{(1)}||y^{(2)}|| \ldots ||y^{(n)}$;
    if $(EQ_x(y) == 1)$
      return y;
    }

Notation: Let q_B be the number of calls to B_x, q_E be the number of calls to EQ_x, ϵ be the advantage for B_x, n the length of the strings and t the running time of $RECOVER^{B_x, EQ_x}(1^n)$. We have the following:

Theorem: Let m be a parameter and $M = 2^m$. There is an algorithm, A which makes $q_B = nM$ calls to B_x, $q_E = M$ calls to EQ_x and runs in time $t = O(nM^2)$ which determines x with probability at least $1 - \delta, \delta = \frac{n}{\epsilon^2 M}$.

First some lemmas and notation. Let $R = \langle r_1, \ldots, r_m \rangle$ and $X_1, X_2, \ldots, X_M : S \rightarrow R$ be a set of real valued random variables on the sample space S.

Lemma 1: If $X_1, X_2, \ldots, X_M : S \rightarrow R$ are pairwise independent and $X = X_1 + X_2 + \ldots + X_M$ then $Var(X) = Var(X_1) + Var(X_2) + \ldots + Var(X_M)$.

Proof: $Var(X) = E(X^2) - E(X)^2 = E(\sum_{i,j} X_i X_j) - \sum_{i,j} E(X_i)E(X_j) = \sum_i [E(X_i^2) - E(X_i)^2] - \sum_{i \neq j} [E(X_i X_j) - E(X_i)E(X_j)]$. The final bracketed sum is 0 by pairwise independence.

Lemma 2: If $X_1, X_2, \ldots, X_M : S \to R$ are pairwise independent, $X = X_1 + X_2 + \ldots + X_M$ and $\mu = E(X) = \sum_{i=1}^{M} E(X_i)$ then $Pr(|x - \mu| \geq A) \leq \frac{\sum_{i=1}^{M} Var(X_i)}{A^2}$.

Proof: By Chebychev, $Pr(|X - \mu| \geq A) \leq \frac{Var(X)}{A^2}$ and by the previous lemma, $Var(X) = Var(X_1) + Var(X_2) + \ldots + Var(X_M)$.

Lemma 3: Let $M = 2^m$. For any $z \in \{0,1\}^n$, $Pr(STRONG - SC^{B_x}(z, r_1, \ldots, r_m, b_1, \ldots, b_m) \neq (z, x)) \leq \frac{1}{M\epsilon^2}$.

Proof: For $R = \langle r_1, r_2, \ldots, r_m \rangle$ and $S_1, S_2, \ldots, S_{2^m}$ a fixed enumeration of $[m]$, define a random variable $X_i(R) = 1$ if $B_x(z + R[S_i]) = (x, z) + b[S_i]$ and 0 otherwise. $X_i(R)$ and $X_j(R)$ are pairwise independent since there is an $r_l \in R$ that is included in *either* the sum $R[S_i]$ or $R[S_j]$ but not both. $E(X_i) = Pr(z + R[S_i] \in Gd_B) = \frac{1+\epsilon}{2}$. Since $E(X_i^2) = E(X_i)$, $Var(x_i) = E(X_1^2) = E(X_i)^2 = E(X_i) - E(X_1)^2 = E(X_1)(1 - E(X_i)) = \frac{1+\epsilon}{2}\frac{1-\epsilon}{2} = \frac{1-\epsilon^2}{4}$. Note that $\mu = \frac{M(1+\epsilon)}{2}$ and so by the previous lemma, $P(X < \frac{M}{2}) = P(|X - \mu| > \frac{M\epsilon}{2}) \leq \frac{M(1-\epsilon^2)/4}{(M\epsilon/2)^2} \leq \frac{1}{M\epsilon^2}$.

Proof of Theorem: Let $M = 2^m$. For any $z \in \{0,1\}^n$, $Pr(RECOVER^{B_x, EQ_x}(1^n) \neq x) \leq \frac{n}{M\epsilon^2}$.

Proof: The loop in $RECOVER$ calls $STRONG - SC^{B_x}$ n times. Each call is wrong with probability at most $\frac{1}{M\epsilon^2}$ so the probability that $RECOVER$ returns the wrong answer is at most $\frac{n}{M\epsilon^2}$.

Note that obtaining x with $p = \frac{1}{2}$ occurs with $M = 2n\epsilon^{-2}$ and the running time is $O(n^3\epsilon^{-4})$ with $q_B = O(n^2\epsilon^{-2})$ and $q_E = O(n\epsilon^{-2})$.

Chapter 3

Cryptography and Computer Security

3.1 Classical Systems

Shannon Theory: Shannon *entropy* of random variable X is $H(X) = -\sum_{i=1}^{n} P(X = x_i) lg(P(X = x_i))$. What is the amount of information in a number $n : 0 \leq n < 2^m$? Information learned about Y by observing X is $I(Y;X) = H(Y) - H(Y|X)$. Note $H(Y|X) = -\sum p_X(x) H(Y|X = x)$ which is generally not equal to $\sum_{X,Y} p_Y(y|x) lg(p_Y(y|x))$. $H_E = lim_{N\to\infty} \frac{H(P^n)}{n}$. $H(K|C) = H(M|C) + H(K|M,C)$.

Application to cryptography: *Perfect secrecy:* $Pr(M|C) = P(M)$. *Unicity Theorem:* Let H be the entropy of the source (say English) and let Σ be the alphabet. Let K be the set of (equiprobable) keys, then $u = \frac{lg(|K|)}{(lg(|\Sigma|)-H)}$. The "Index of Coincidence," $IC(f) = \frac{\sum f_i(f_i-1)}{n(n-1)}$. $MC(f,f') = \frac{\sum f_i f'_i}{nn'}$.

Vigeniere alphabet chaining: If α is the mixed plaintext alphabet and β is the mixed cipher alphabet underneath, rearranging with the plain alphabet into its normal form we get the tableaux:

1	2	...	n
$\beta(\alpha^{-1}(1))$	$\beta(\alpha^{-1}(2))$	...	$\beta(\alpha^{-1}(n))$
$\beta(\alpha^{-1}(1)+1)$	$\beta(\alpha^{-1}(2)+1)$	...	$\beta(\alpha^{-1}(n)+1)$
...	...	...	...
$\beta(\alpha^{-1}(1)+n-1)$	$\beta(\alpha^{-1}(2))$	...	$\beta(\alpha^{-1}(n)+n-2)$

Note that the columns have the same sequence of characters as the original rows — if plain A corresponds to cipher F and if plain F corresponds to cipher W then the distance between plain A and plain F is the same as cipher F and cipher W in the original sequence.

Heburn: Five rotors, two ratchet controls. Key: $[i,j,k,m,n]$ and 2 ratchet stepping controls at right and left (l,r). Rightmost (R_5) rotor moved after every enciphered letter. Leftmost (R_1) moved when fast rotor reached position specified by r. $a(m)$ character in line to R_5. When the leftmost rotor hit l the middle (R_3) rotor moved one position. Equation: $(p)KC^iR_1C^{-i}C^jR_2C^{-j}C^kR_3C^{-k}C^mR_4C^{-m}C^nR_5C^{-n}L = c$, C is the cyclic in alphabetical order. Solution: $c(m) = a(m)C^{(m+p)}R_5C^{-(m+p)}L$, $d(m,p) = c(m)L^{-1}C^{(m+p)}R_5^{-1}C^{-(m+p)}$ then $d(m,p)R_5^{-1}C^{n-m}R_5 = d(n,p)$. Practical application relies on the IC for the monoalphabetic substitution (imagine all the input letters are the same). If $i = d(m,p)$, $j = d(n,p)$ and $k = n-m$. To remove noise, tally $s'[i,j,k] = \sum_m \sum_n s[i,m,k-m]s[m,j,n]$, this can be iterated.

Enigma: K: Keyboard. $P = (ABCDEFGHIJKLMNOPQRSTUVWXYZ)$. N: First Rotor. M:

Second Rotor. L: Third Rotor. U: Reflector. Note: $U = U^{-1}$. i, j, k: Number of rotations of first, second and third rotors respectively. $c = (p)P^iNP^{-i}P^jMP^{-j}P^kLP^{-k}UP^kL^{-1}P^{-k}P^jM^{-1}P^{-j}P^iN^{-1}P^{-i}$. Later military models added plug-board or "Stecker"(S):

$$c = (p)SP^iNP^{-i}P^jMP^{-j}P^kLP^{-k}UP^kL^{-1}P^{-k}P^jM^{-1}P^{-j}P^iN^{-1}P^{-i}S^{-1}.$$

Total key including rotor wiring (in bits): $67.1 + 3 \times 88.4 = 312.3$.
Method of Batons (no Stecker): Let N be the fast rotor and Z the combined effect of the other apparatus, then, $N^{-1}ZN(p) = c$ at first letter; assuming other rotor doesn't turn, $P^{-i}N^{-1}P^iZP^{-i}NP^i(p) = c$ or $ZP^{-i}N(p(i))P^i = P^{-i}NP^ic(i)$. *Rejewski:* Let $Q = MLUL^{-1}M^{-1} = Q^{-1}$, the first 6 permutations (used to encrypt settings twice) are:

$$A = A^{-1} = SP^1NP^{-1}QP^1N^{-1}P^{-1}S^{-1}, B = B^{-1} = SP^2NP^{-2}QP^2N^{-1}P^{-2}S^{-1}$$

$$C = C^{-1} = SP^3NP^{-3}QP^3N^{-1}P^{-3}S^{-1}, D = D^{-1} = SP^4NP^{-4}QP^4N^{-1}P^{-4}S^{-1}$$

$$E = E^{-1} = SP^5NP^{-5}QP^5N^{-1}P^{-5}S^{-1}, F = F^{-1} = SP^6NP^{-6}QP^6N^{-1}P^{-6}S^{-1}$$

Their products and ciphertext ($c_1c_2c_3c_4c_5c_6$) satisfy:

$$AD = SP^1NP^{-1}QP^1N^{-1}P^3NP^{-4}QP^4N^{-1}P^{-4}S^{-1}, (c_1)AD = c_4$$

$$BE = SP^2NP^{-2}QP^2N^{-1}P^3NP^{-5}QP^5N^{-1}P^{-5}S^{-1}, (c_2)BE = c_5$$

$$CF = SP^3NP^{-3}QP^3N^{-1}P^3NP^{-6}QP^6N^{-1}P^{-6}S^{-1}, (c_3)CF = c_6$$

So we can find AD, BE and CF after about 80 messages. To solve for rotors if S is known. First note the following theorem.

Theorem: If two permutations of the same degree consist of disjoint transpositions then their product contains an even number of cycles of the same length (and conversely). "Cillies" (guessed simple indicators like aaa) align cycles. Let $U = P^{-1}S^{-1}ASP = PNP^{-1}QPN^{-1}P^{-1}$, $V = P^{-2}S^{-1}BSP^2$, etc, then $VW = NP^{-1}N^{-1}(UV)NPN^{-1}$, $WX = NP^{-1}N^{-1}(VW)NPN^{-1}$, etc. which can be solved for N.

Assume we know all rotor wirings and the plaintext for some received ciphertext. We do not know plugboard, rotor order, ring and indicator.

```
Position   12345678901234567890123
Plain Text OBERKOMMANDODERWEHRMACHT
CipherText ZMGERFEWMLKMTAWXTSWVUINZ
```

Observe the loop $A[9] \to M[7] \to E[14] \to A$. $(E)M_7M_9M_{14} = E$, where M_i is the effect of the machine at position i. British Bombe searched probable text for these loop isomorphisms. False alarms have probability $\frac{1}{26}$ for each independent loop tested.

3.2 Public Key Systems

RSA: $n = pq$, choose e, $ed = 1 \pmod{\phi(pq)}$, e is often $2^{16} + 1$ for efficiency.

DLP: Given g, h and $h = g^x$, find x. **DHP:** Given $g, a = g^x, b = g^y$, find $z = g^{xy}$. **DDH:** Given $g \in G, a = g^x, b = g^y, c = g^z$, determine if $z = xy$. $DDH \leq DHP \leq DLP$.

Theorem: $FACTOR \leq SQRT \leq FACTOR$. If the RSA problem is hard, then RSA is secure under a chosen plaintext attack. If DHP is hard, El Gamal is secure under a chosen plaintext attack.

Finding square roots (mod p): Suppose $(\frac{a}{p}) = 1$, so that a is a square and let n be a quadratic non-residue (mod p). Want to find x: $x^2 = a \pmod{p}$. Set $p-1 = 2^e q$ and put $b = n^q \pmod{p}$ If $p = 3 \pmod{4}$, $x = a^{\frac{(p+1)}{4}} \pmod{p}$. If $p = 5 \pmod{8}$, let $b = a^{\frac{(p-1)}{4}} = \pm 1 \pmod{p}$, then if $b = 1, x = a^{\frac{(p+3)}{8}} \pmod{p}$, otherwise, if $b = -1, x = (2a)(4a)^{\frac{(p-5)}{8}} \pmod{p}$. This leaves the hard case, $p = 1 \pmod{8}$). The algorithm of *Tonelli and Shanks* solves this case (and the others). We want $x : x^2 = a \pmod{p}$. Put $p-1 = 2^e q$, q, odd. Choose n: $(\frac{n}{p}) = -1$; note n is a generator for the multiplicative group. Set $z = n^q \pmod{p}$ and $b = a^q$. Since $b^{2^{e-1}} = 1$, b is a quadratic residue and $b = z^{2k}$ or $bz^{k'} = 1$. Put $x = a^{\frac{q+1}{2}} z^{\frac{k'}{2}}$ then $x^2 = a \pmod{p}$. The algorithm:

$Q = \frac{(q-1)}{2}$, $z = n^q$, $y = z$, $r = e$, $x = a^Q \pmod{p}$, $b = ax^2 \pmod{p}$ and $x = ax \pmod{p}$. $x = a^{\frac{q+1}{2}} z^{\frac{k'}{2}}$ will satisfy $a = x^2$ where $z^k = 1$. Now set $R = 2^{r-1}, ab = x^2, y^R = -1, b^R = 1$. Do the following:

loop:
  if($b = 1$)
    return(x);
  Let $M = 2^m$. For smallest $m > 0 : b^M = 1 \pmod{p}$
  if($m = r$)
    return(non-residue);
  $t = y^{2^{r-m-1}} \pmod{p}$;
  $y = t^2 \pmod{p}$;
  $r = m$;
  $x = xt$;
  $b = by$;
  goto loop;

Theorem: Factoring n may be equivalent to computing $\phi(n)$ which is equivalent to finding d.

Definitions: *Strong primes:* $p-1$ has a large prime factor r, $p+1$ has a large prime factor a, $r-1$ has a large prime factor t. *Miller-Rabin* has error probability $p = \frac{1}{4}$ as the following shows.

Definition: A composite number n is a Carmichael number if $\forall a < n : (a, n) = 1$ we have $a^{n-1} = 1 \pmod{n}$.

Theorem: $n \geq 3$ is a Carmichael number iff n is square-free and $(p-1) \mid (n-1), \forall p | n$.

Proof: Let $(a, n) = 1$.
$\rightarrow$: Suppose n is a Carmichael number. $a^{p-1} = 1 \pmod{p}$ so $a^{p-1} = 1 \pmod{n}$ and $(p-1) \mid (n-1)$. If n is not square free, $p^k(p-1) \mid \phi(n)$ so, for some a, $a^p = 1 \pmod{n}$ but $a^{p-1} = 1 \pmod{n}$. Contradiction.
$\leftarrow$: Suppose n is square-free and $(p-1) \mid (n-1), \forall p \mid n$. $a^{p-1} = 1 \pmod{p}$. So $a^{n-1} = 1 \pmod{n}$.

Theorem: If $n \geq 3$ is a Carmichael number, n is divisible by three or more primes.

Proof: Suppose $n = pq$. $(p-1) \mid (pq-1)$ and $(q-1) \mid (pq-1)$. $(p-1)a = pq-1 = pq-q+q-1 = q(p-1)+q-1$ so $(p-1) \mid (q-1)$. Thus $2(p-1) \geq (q-1)$. Similarly $2(q-1) \geq (p-1)$. This is a contradiction.

Theorem: If n is prime, $n-1 = 2^s d$ $\forall a < n$, then either $a^d = 1 \pmod{n}$ or $a^{2^r d}$ for some $r < s$.

Proof: For any $a : (a, n) = 1$, $a^{2^s d} = 1 \pmod{n}$ and the result follows.

Theorem: If $n \geq 3$ is composite then $S = \{x : 1 \leq x < n\}$ has at most $\frac{n-1}{4}$ non-witnesses.

Proof: If there are no non-witnesses, the result holds. Let a be a non-witness, $a^d = 1 \pmod{n}$ or $a^{2^r d} = -1 \pmod{n}$ for some $r < s$. In fact, we can assume $a^{2^r d} = -1 \pmod{n}$ because $a^d = 1 \pmod{n}$ implies $(-a)^d = -1 \pmod{n}$. Let k be the largest $k : a^{2^k d} = -1 \pmod{n}$. Put $n = \prod_{p|n} p^{e_p}$ and $m = 2^k d$. Define $J = \{a, a < n, (a, n) = 1, a^{n-1} = 1 \pmod{n}\}$, $K = \{a, a < n, (a, n) = 1, a^{n-1} = \pm 1 \pmod{p^{e_p}}\}$, $L = \{a, a < n, (a, n) = 1, a^m = \pm 1 \pmod{n}\}$, and $M = \{a, a < n, (a, n) = 1, a^m = 1 \pmod{n}\}$. Thus $M \subseteq L \subseteq K \subseteq J \subseteq (\mathbb{Z}/(n\mathbb{Z}))^*$. If a is a non-witness, $a \in L$. $[K : M] = 2^\alpha$ since $x \in K \to x^2 \in M$. So $[K : L] = 2^j$. If $j \geq 2$, we're done. If $j = 1$, $n = pq$ and n is not a Carmichael number, so $[(\mathbb{Z}/(n\mathbb{Z}))^* : K] \geq 1$. $[K : L] = 2$ so $[(\mathbb{Z}/(n\mathbb{Z}))^* : L] \geq 4$ and we're done. If $j = 1$, $n = p^e, e > 1$ so $p(p-1) \mid \phi(n)$ and $[(\mathbb{Z}/(n\mathbb{Z}))^* : J] \geq p$. If $p^e \geq 4$, were done. The only remaining case is $n = 9$. The theorem holds for this case as well.

El Gamal Crypto: For the *El Gamal encryption system*, let g be a generator of F_q^*. A picks a at random, this is A's secret. User picks k at random and sends (g^k, Pg^{ka}). An *El Gamal Signature* is generated as follows: g is a primitive element $\mathbb{Z}_p^*$. $(p, g, y = g^x)$ are public, x is secret. To sign m, pick k: $1 \leq k \leq p-2$ with $(k, p-1) = 1$. $sig_K(m, k) = (r, s)$, $r = g^k$, $s = k^{-1}(m - xr)$. $ver_k(m, r, s)$ is true iff $y^r r^s == g^m$. Note: k must be different for each signature and m must be a hash. *Recommended parameters:* > 768 bits. There is an existential forgery if hash isn't used in El Gamal. For key elements, $(\langle \mathbb{Z}_p \rangle, g, a)$, pick (u, v), $r = g^u g^v = g^{u+av}$. $s = -rv^{-1} \pmod{p-1}$, $M = su$. Note that $t = r^s y^r = g^{su}$.

Diffie Hellman Key Exchange: The *Diffie Hellman* key exchange scheme works as follows: Let g be a generator of F_q^*. A generates $a \in F_q^*$ at random and transmits g^a, B generates $b \in F_q^*$ at random and transmits g^a, they use g^{ab} as key.

Blinding and E-cash: Let M be a note or check. To blind, generate random k. Let (e, d, n) be the bank's key and H, a hash. Send bank $r = H(M)k^e$. Bank sends back r^d, now multiply by k^{-1}. For fraud resistant protocol, do this for a bunch of k_s's. Bank signs one of them.

DSA: Pick p, q, $2^{159} < q < 2^{160}$, $2^{511+64t} < p < 2^{512+64t}$, $0 \leq t \leq 8$ with $q|(p-1)$. Let x be a primitive root $\pmod{p}$. Set $g = x^{\frac{p-1}{q}} > 1 \pmod{q}$. Finally, pick a at random and set $A = g^a \pmod{p}$. p, q, g, A are public, a is secret. To sign M: generate random $k : k < q$. Set $r = g^k \pmod{q}$ and compute $s = k^{-1}(h(M) + xr) \pmod{q}$, where h is a cryptographic hash. *Signature* is (r, s). *To verify:* $u_1 = s^{-1}h(M) \pmod{q}$, $u_2 = s^{-1}r \pmod{q}$, $v = g^{u_1} g^{u_2} \pmod{p} \pmod{q}$. If $v = r$, it verifies. Unlike El Gamal signature, s does not carry full information about p (only $\pmod{q}$) and since q is large, the Pohlig-Hellman attack is harder.

Montgomery Arithmetic: Suppose $(R, n) = 1$; think of $R = 2^r$, $n < 2^r$. $RR' - nn' = 1$ (i.e.- $n' = -n^{-1} \pmod{R}$).
Theorem: If $0 \leq t < nR$ and $u = tn' \pmod{R}$ then $R \mid (t + un)$ and for $x = \frac{(t+un)}{R}$, $x = tR^{-1} \pmod{n}$ and $0 \leq x < 2n$.

$\overline{a} = ar \pmod{n}$. $rr' - nn' = 1$.
MontPro$(\overline{a}, \overline{b})$
$t = \overline{a}\overline{b}$;

$u = tn' \pmod R$;
$x = \frac{un+t}{R}$;
if$(x > n)$
$x- = n$;
return(x);

MontMult(a, b, n): Compute n' ;
$\overline{a} = ar \pmod n$;
$\overline{b} = br \pmod n$;
$\overline{x} = MontPro(\overline{a}, \overline{b})$;
$x = MontPro(\overline{x}, 1)$;
return(x).

NAF: Let $k = \sum_{j=0}^{l} s_j 2^j, s_j \in \{0, 1\}$. NAF form is $k = \sum_{j=0}^{l+1} c_j 2^j, c_j \in \{-1, 0, 1\}$, conversion is achieved by following algorithm:

$c_0 = 0$;
$for(j = 0; j \leq l; j++)\{$
$c_{j+1} = \lfloor (k_j + k_{j+1} + c_j)/2 \rfloor$;
$s_j = k_j + c_j - 2c_{j+1}$;
}

AMD-64 3Ghz dual core timings:

Algorithm	KSize	T(μ-sec)	Cycles	Algorithm	KSize	T(μ-sec)	Cycles
ECDSA-SIGN	256	4942	14,827,000	ECDSA-VERIFY	256	9,848	29,546,000
ECDSA-SIGN	384	13,000	38,860,000	ECDSA-VERIFY	384	25,900	77,639,000
ECDSA-SIGN	521	29,500	88,287,000	ECDSA-VERIFY	521	58,900	176,524,000

Algorithm	KeySize	T(μ-sec)	Cycles	Algorithm	KeySize	T(μ-sec)	Cycles
DSA-SIG	512	1,077	3,233,000	DSA-VERIFY	512	2,142	6,427,000
DSA-SIG	768	2,332	6,999,000	DSA-VERIFY	768	4,641	13,924,000
DSA-SIG	1024	4,027	12,083,000	DSA-VERIFY	1024	8,015	24,047,000

Algorithm	KeySize	T(μ-sec)	Cycles	Algorithm	KeySize	T(μ-sec)	Cycles
RSA-SIGN	1024	3,488	10,465,000	RSA-VERIFY	1024	168	505,000
RSA-SIGN	2048	22,905	68,717,000	RSA-VERIFY	2048	608	1,825,000
RSA-SIGN	3072	72,494	217,491,000	RSA-VERIFY	3072	1,340	4,021,000
RSA-SIGN	4096	168,548	505,664,000	RSA-VERIFY	4096	2,363	7,091,000

Algorithm	KeySize	T(sec)	Algorithm	KeySize	T(sec)
RSA KeyGen	1024	.37	ECC KeyGen	160	.0053
RSA KeyGen	2048	3.5	ECC KeyGen	224	.0056
RSA KeyGen	3072	11.2	ECC KeyGen	256	.0067

McEliece Cryptosystem: Bob chooses G, an $[n, k, d]$ linear code, $G_1 = SGP$ where P is an $n \times n$ permutation matrix and S is a $k \times k$ invertible matrix. To send a message to Bob, Alice adds an error, e, of weight t, $y = xG_1 + e$. To decrypt, (1) compute $y_1 = yP^{-1} = xSG + e_1$; (2) apply error decode to y_1 to get x_1; (3) compute $x_0 : x_0G = x_1$; (4) compute $x = x_0S^{-1}$. Want d to be large. For example, use Goppa code

$(n = 2^m, d = 2t + 1, k = n = mt)$: $m = 10, t = 50$ to get $[1024, 524, 101]$.

3.3 Symmetric Key Systems

Modes: *CBC:* $y_0 = IV$, $y_i = E_K(x_i + y_{i-1})$.
OFB: $z_0 = IV$, $z_{i+1} = E_K(z_i)$, $y_i = x_i + z_i$.
CFB: $y_0 = IV$, $z_i = E_K(y_{i-1})$, $y_i = x_i + z_i$.
CTR: $z_i = E_K(Nounce||ctr)$, $y_i = x_i \oplus z_i$.
HMAC: $(K, m) \mapsto h((K \oplus a)||h(K \oplus b)||m)$.
GCM: $F = GF(2^{128}), p(x) = 2^{128} + x^7 + x^2 + x + 1$, $(z_0, y_0) = (IV, 0^{128})$, $(z_1, y_i) \mapsto (z_{i+1}, y_{i+1})$ by $z_{i+1} = \pi_i(z_i)$, if $\pi_i(x) = 0$, $z_i \oplus y_i$ otherwise and $y_{i+1} = y_i >> 1$ if $LSB(y_i) = 0$ otherwise $y_{i+1} = (y_i >> 1) \oplus R$, $R = [11100001||0^{120}$. Define $X \cdot Y = (z_{128}, y_{128})$. $inc_s(X) = MSB_{len(X)-s}(X)||[int(LSBs(X)) + 1 \pmod{2^s}]_s$. $GHASH_H(X), len(X) = 128m$: $H = E_K(0^{128})$. $Y_0 = 0^{128}$, $Y_{i+1} = (Y_i \oplus X_{i+1}) \cdot H$. return Y_m.
GCTR: $GCTR_K(ICB, X)$: If X is the empty string, then return the empty string as Y. $n = \lceil (len(X)/128 \rceil$. Let $CB_1 = ICB$, $CB_i = inc_{32}(CB_{i-1}, i = 1 \ldots n$. $Y_i = X_i \oplus E_K(CB_i)$. ${Y_n}^* = {X_i}^* E_K(CB_i)$. return Y.
GCM-AES: $GCM - AE_K(IV, P, A)$: $H = E_K(0^{128})$. If $len(IV) = 96$, $J_0 = IV||0^{31}||1$. If $len(IV) \neq 96$, let $s = 128\lceil len(IV)/128 \rceil - len(IV)$, and let $J_0 = GHASH_H(IV||0^{s+64}||len(IV)^{64})$. $C = GCTR_K(inc_{32}(J0), P)$. Let n Define $S = GHASH_H(A||0^v||C||0^u||len(A)^{64}||len(C)^{64})$. $T = MSB_t(GCTR_K(J_0, S))$. return (C, T).

Definitions: *Recurrence for LFSR of length k:* $s_j = c_1 s_{j-1} + \ldots c_k s_{j-k}$. *Hamming weight:* $w_H(x) = \#\{n : x_n \neq 0\}$. *Modular weight:* $w_M(x) = |x'|$ where $x' = x \pmod{2^n}$ and $-2^{n-1} < x' \leq 2^{n-1}$. *NAF weight:* $w_{NAF}(x) = \#\{i < n : \alpha_i \neq 0\}$. $\Delta^{\oplus}(x, y)$, $\Delta^{+}(x, y)$, $\Delta^{\pm}(x, y)$ are the xor, modular and signed differences respectively. *Distortion for map* φ: $D(\varphi, d_1, d_2) = sup_{x \neq y} \frac{d_2(\varphi(x), \varphi(y))}{d_1(x,y)} sup_{x \neq y} \frac{d_1(x,y)}{d_2(\varphi(x), \varphi(y))}$. $f(x_1, \ldots, x_n)$ is *m-correlation immune* if $I(f(x_1, \ldots, x_n); x_{i_1}, \ldots, x_{i_m}) = 0$ for any choice of the i_k. This happens when the boolean spectrum of $F(w)$ is 0 when w has weight $\leq m$.

Definition: The *connection polynomial* for $L_n(\vec{s})$ is $c(x) = 1 + c_1 x + \ldots + c_l x^l$ with $c(x) = 0$ if $L_n(\vec{s}) = 0$. Define d_n as nth discrepancy, suppose m is the position of change of length in minimal generating LFSR. $L_m(\vec{s}) \leq L_n(\vec{s})$ and $L_{m+1}(\vec{s}) = L_n(\vec{s})$. The recurrence is $c^{(n+1)}(x) = c^{(n)}(x) - d_n {d_m}^{-1} x^{n-m} c^{(m)}(x)$. The synthesis algorithm is $O(n^2)$.

Theorem: A LFSR of length k has maximal period ($K = 2^k - 1$) iff its connection polynomial is *primitive*.

Proof: Let $G(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{m-1} x^{m-1} + \ldots$, $a_m = c_1 a_{m-1} + \ldots + c_m a_1$, etc. We get a recurrence yielding $\frac{K}{1 - c(x)}$, $f(x) = 1 - c(x)$. If sequence is p, $G(x) = (a_0 + a_1 x + \ldots + a_{m-1} x^{m-1}) + (a_0 + a_1 x + \ldots + a_{m-1} x^{m-1}) x^p + \ldots = \frac{(a_0 + a_1 x + \ldots + a_{m-1} x^{m-1})}{1 - x^p} = \frac{K}{(f(x))}$.

Theorem: Let $M_{j,k}(x) = \begin{pmatrix} x_j & x_{j+1} & x_{j+2} & \ldots & x_{j+k-1} \\ x_{j+1} & x_{j+2} & x_{j+3} & \ldots & x_{j+k} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ x_{j+k-1} & x_{j+k} & x_{j+k+1} & \ldots & x_{j+2k-2} \end{pmatrix}$. If $\langle x_i \rangle$ is generated by an LFSR of length N but not one shorter then $det(M_{j,N}(x)) = 1$ and $det(M_{j,n}(x)) = 0, n > N$. If $x_{n+m} = c_0 x_n + \ldots + c_{m-1} x_{n+m-1}$ and $c(x) = x^m + c_{m-1} x^{m-1} + \ldots + c_0$, the associated connection polynomial, is irreducible, then the sequence repeats at an interval of $k = 2^m - 1$.

Massey's Lemma: If $L_n(\vec{s})$ generates $\langle s_0, \ldots, s_{n-1}\rangle$ but not $\langle s_0, \ldots, s_n\rangle$ then $L_{n+1}(\vec{s}) \geq max(L_n(\vec{s}), n + 1 - L_n(\vec{s}))$.

Proof: Suppose L generates $\langle s_0, s_1, \ldots, s_{n-1}\rangle$ but not $\langle s_0, s_1, \ldots, s_n\rangle$ and let L' with $L'_{n+1}(\vec{s}) = l'$ then $l' \geq n + 1 - l$. Proof. If $l \geq n$, $l' \geq 1$ so it's true. If $l < n$, let c_i be the coefficients of L and c'_i, the coefficients of L'. $s_j + \sum_{i=1}^{l} c_i s_{j-i} = 0$ for $j = l, l+1, \ldots, n-1$ but not for $j = n$ and $s_j + \sum_{i=1}^{l'} c'_i s_{j-i} = 0$ for $j = l', l'+1, \ldots, n$ so $-\sum_{i=1}^{l} c_i s_{j-i} = \sum_{i=1}^{l} c_i \sum_{k=1}^{l'} c'_k s_{n-i-k}$ Switching the order of summation, the second sum is s_n which is a contradiction.

Berlekamp-Massey: Given $s_1, s_2, \ldots, s_{n-1}$ output linear complexity L.

1. $C(x) = 1, L = 0, m = -1, b(x) = 1, n = 0$.
2. $d = S_n + \sum_{i=1}^{L} c_i s_{n-i}$.
3. If $(d == 1)$ $t(x) = c(x), c(x) += b(x)x^{n-m})$ if$(L \leq \frac{n}{2})$ $L = n + 1 - L, m = n, b(x) = t(x)$
4. $n = n + 1$;

```
RC4Init() {
    for (i=0; i<256; i++)
        s[i]= i;
    fill k[] with key repeating
         as necessary;
    j= 0;
    for(i = 0; i<256; i++) {
        j= (k[i]+s[i]+j) (mod 256);
        swap(s[i], s[j]);
        }
        i= 0;
        j= 0;
        }

byte Next() {
        i= (i+1) (mod 256);
        j= (j+s[i]) (mod 256);
        swap(s[i], s[j]);
        return(s[(s[i]+s[j]) (mod 256)]);
        }
```

Let $\Lambda(s^n)$ be the associated *linear complexity* of the sequence $\langle s_i\rangle$ of length n and $N_n(L)$ be the number of sequences of length n with linear complexity L, then $N_n(L) = 2N_{n-1}(L) + N_{n-1}(n - L)$, if $n \geq L > \frac{n}{2}$; $N_n(L) = 2N_{n-1}(L)$, if $L = \frac{n}{2}$; and, $N_n(L) = N_{n-1}(L)$, if $\frac{n}{2} \geq L \geq 0$. So $N_n(L) = 2^{min(2n-2L, 2L-1)}$, if $n \geq L > 0$, $N_n(L) = 1$, if $n \geq L = 0$. $E(\lambda(s^n)) = \frac{n}{2} + \frac{4+R_2(n)}{18} - 2^{-n}(\frac{n}{3} + \frac{2}{9})$, $Var(\Lambda(s^n)) = \frac{86}{81}$.

Shrinking Generator: Take two LFSR: $LFSR_1$ and $LFSR_2$ synchronously clocked. Use $LFSR_2(t)$ in stream when $LFSR_1(t) = 1$. Take $LFSR_i(t) = x_i(t)$ for $i = 1, 2, \ldots, n$ use $f(x_1(t), x_2(t), \ldots, x_n(t))$ where f is non linear. For k stage shift register design, where stage i has n_i bits of state, keysearch takes $2^{n_0+n+1+\ldots+n_{k-1}}$ while correlation attack takes $2^{n_0} + 2^{n+1} + \ldots + 2^{n_{k-1}}$. *Example:* The Geffe combiner is $f(x, y, z) = xy \oplus yz \oplus z$, $f(x, y, z) = x$ with $p = \frac{3}{4}$.

ANSI 9.17 random stream generator: $I = E_k(D)$. $x_i = E_k(I \otimes s)$ and $s = E_k(x_i \otimes s)$.

FIPS 186 One Way Function (OWF): t, c 160 bits. Output $G(t, c)$ where $t = H_1||H_2 \ldots ||H_5$. Pad c with 0s to get 512 bit block X. Break X into 16 32 bits words $x_0, \ldots, x_{15}$ and set $m = 1$, apply iterative step of SHA-1.

```
Dual Elliptic Curve RNG
  s[0] in [0,1, ..., #E-1]
  output 240 bits
  for(i=1 to k {
    s[i]= x(s[i-1]P);
    r[i]= lsb[240] x(s[i]Q);
    }
  return(r[1] ... r[k]);

// State for Hash_DRBG
  V // seedlen bits
  C // seedlen bits
  reseedCtr

Hash_DRBG_Instantiate(entBitsIn, nonce,
                      extraEnt)
  seedBits= entBitsIn||nonce||extraEnt;
  seed= Hash_df(seedBits, seedlen);
  V= seed;
  C= Hash_df((0x00||V), seedlen);
  reseedCtr= 1;
  return;

Hash_DRBG_Reseed(entBitsIn, addInBits)
  seedBits= 0x01||V||entBitsIn||addInBits;
  seed= Hash_df(seedBits, seedlen);
  V= seed;
  C= Hash_df((0x00||V), seedlen);
  reseedCtr= 1;
  return;

Hash_DRBG_Generate(numReqBits, addInBits)
  if(reseedCtr>reseedInterval) then
       Reseed;
  if(addInBits!=NULL)
     w= Hash(0x02||V||addInBits);
     V=(V+w) mod 2**seedlen;
  returnedBits= Hashgen(numReqBits, V);
  H= Hash(0x03||V);
  V=(V+H+C+reseedCtr) mod 2**seedlen;
  reseedCtr= reseedCtr+1;
  return returnedBits;

Hashgen(numReqBits, V)
  m= reqNumBits/outlen;
  data= V;
  W= NULL;
  for i= 1 to m
    w= Hash(data);
    W= W||w;
    data= (data+1) mod 2**seedlen;
  returnedBits= Leftmost numReqBits
                bits of W;
  return returnedBits;

Hash_df(inBits, numRetBits):
  temp= NULL;
  m= numRetBits/outlen;
  counter= 8-bit representation of 1;
  for i= 1 to len do
    temp= temp|| Hash(counter||
            numRetBits||inBits);
    counter= counter+1;
  reqBits= Leftmost numRetBits of temp;
  return reqBits;

// State for CTR_DRBG
    V // outlen bits
    C // keylen bits
    reseedCtr
    nStrength
    fPrediction

CTR_DRBG_Update(provided_data, Key, V):
  temp= NULL;
  while(len(temp)<seedlen) do
    V=(V+1) mod 2**outlen;
    outBits= blockEncrypt(Key, V);
    temp= temp||ouput_block;
  temp= Leftmost seedlen bits of temp;
  temp= temp^provided_data;
  Key= Leftmost keylen bits of temp;
  V= Rightmost outlen bits of temp;
  return Key and V;

// Full Entropy
CTR_DRBG_Instantiate(entBitsIn, extraEnt):
  // Ensure that the length of
  // extraEnt is seedlen bits.
  temp= len(extraEnt);
  if(temp<seedlen))
    extraEnt= extraEnt||
                [seedlen-temp] bits of 0;
  seedBits= entBitsIn^extraEnt;
  Key= [keylen] bits of 0;
  V= [outlen] bits of 0;
  (Key, V)= Update (seedBits, Key, V);
  reseedCtr= 1;
  return;
```

```
// Derivation function required
CTR_DRBG_Instantiate(entBitsIn, extraEnt):
  seedBits= entBitsIn||nonce||extraEnt;
  seedBits= Block_Cipher_df(seedBits, seedlen);
  Key= 0 of[keylen];
  V= 0 of[outlen];
  (Key, V)= Update (seedBits, Key, V);
  reseedCtr= 1;
  return;

// Full entropy
CTR_DRBG_Reseed(entBitsIn, addInBits):
  temp= len(addInBits);
  if(temp<seedlen), then
      addInBits= addInBits||
           [seedlen-temp] bits of 0;
  seedBits= entBitsIn^addInBits.;
  (Key, V)= Update (seedBits, Key, V);
  reseedCtr= 1;
  return;

// Derivation Function Required
CTR_DRBG_Reseed(entBitsIn, addInBits):
  seedBits= entBitsIn||addInBits;
  seedBits= Block_Cipher_df(seedBits,
                            seedlen);
  (Key, V)= Update (seedBits, Key, V);
  reseedCtr= 1;
  return;

CTR_DRBG_Generate(numReqBits, addInBits):
    if reseedCtr>reseedInterval, then
            reseed;
    if(addInBits!=NULL)
        temp= len(addInBits);
    if(temp<seedlen))
        addInBits= addInBits||
                 [seedlen-temp] bits of 0;
        (Key, V)= Update (addInBits, Key, V);
    else
      addInBits= [seedlen] bits of 0;
   temp= NULL;
   while(len(temp)<numReqBits) do:
     V=(V+1) mod 2**outlen;
     outBits= blockEncrypt(Key, V);
     temp= temp||outBits;
   returnedBits= Leftmost numReqBits of temp;
   // Update for backtracking resistance.
   (Key, V)= Update(addInBits, Key, V);
   reseedCtr= reseedCtr+1;
   return returnedBits;

BCC(Key, data):
  CV= [outlen] bits of 0;
  n= len(data)/outlen;
  Split the data into n blocks of outlen bits
       forming block[1] to block[n];
  for i= 1 to n do
    inBlock= CV^block[i];
    CV= blockEncrypt(Key,inBlock);
  outBits= CV;
  Return outBits;

Block_Cipher_df(numRetBits, inBits)
  if(numRetBits>maxNumBits), then
    return ERROR;
  L= len(inBits)/8;
  N= numRetBits/8;
  S= L||N||inBits||0x80;
  // Pad S with zeros, if necessary.
  while(len(S) mod outlen) != 0
       S= S||0x00;
  temp= NULL;
  i= 0;
  K= Leftmost keylen bits
         of 0x00010203...1D1E1F.
  while len(temp)<keylen+outlen)
    IV= i||[outlen-len(i)] bits of 0;
    temp= temp||BCC(K,(IV||S));
    i= i+1;
  K= Leftmost keylen bits of temp;
  X= Next outlen bits of temp;
  temp= NULL;
  while len(temp)<numRetBits
    X= blockEncrypt(K, X);
    temp= temp||X;
  reqBits= Leftmost numRetBits of temp;
  return reqBits;
```

MGF property: Given no input and partial output, remaining output is unpredictable.

```
mgf1(mSeed, nLen)
1. if (mLen>2^32), return error
2. T= ||;
3. uL= ceiling(mLen/hLen),
```

```
   // hLen is length of hash used
4. for(c=0; c<uL;c++)
       T= t|| h(mSeed || c);
5. output leading bits
```

```
PSS-Encode(M, emBits, salt, sLen)
// M- message
// emBits- bits of EM >= 8 hLen + 8 sLen + 9
1. emLen= ceil(enBits/8);
2. if (l(M)> largest message), return error;
3. mH= h(M)
4. if( emLen < hLen+sLen+2 ), return error;
5. M'= (0x00)^8 || mH || salt
6. H= h(M');
7. DB= (0x00)^(emLen-hLen-sLen-2)
       || 0x01 || salt
8. dbMask= mgf(H, emLen-hLen-1);
9. maskedDB= DB^dbMask;
10. Clear leftmost 8*emLen-emBits in maskedDB
11. EM= maskedDB || H || 0xbc
12. return EM;
```

```
emsa-pkcs(M, emLen)
// emLen= l(EM)>= tLen+11
1. H= h(M)
2. T= hash-prefix || H ;  // tLen= l(T)
3. EM= 0x00 || 0x01 || (0xff)^(emLen-tLen-3) || T;
4. return EM;
```

Blum-Blum-Shub: Select p, q each $= 3 \pmod 4$, $n = pq$, $s \in [1, n-1]$-seed, $(s, n) = 1$ $x_0 = s^2 \pmod n$ for(i=1 to l) $x_i = x_{i-1}^2 \pmod n$ $z_i = LSB(x_i)$. Next bit test: Given l bits, no polynomial time algorithm can predict the $l+1$st with probability $> \frac{1}{2} + \epsilon$.

```
RC6 input: A,B,C,D, r rounds, w-bit round keys in S[0...2r+3].

RC6() {
    B= B+S[0];
    D= D+S[1];
    for(i=1;i<=r;i++) {
        t= (B*(2B+1)) <<< lg(w);
        u= (D*(2D+1)) <<< lg(w);
        A= ((A^t)<<<u)+S[2i];
        C= ((C^u)<<t)+S[2i+1];
        (A, B, C, D) = (B,C,D,A);
        }
    A= A+S[2r+2];
    C= C+S[2r+3];
    }
```

```
// Key L[0 to k-1];
RoundKeys(L,S,k) {
    S[0]= 0xB7E15163al Elliptic Curve RNG
    s[0] in [0,1, ..., #E-1]
    output 240 bits
    for(i=1 to k {
        s[i]= x(s[i-1]P);
        r[i]= lsb[240] x(s[i]Q);
        }
    return(r[1] ... r[k]);
```

OAEP: Want to send m. Let $\rho(r)$ be a pseudo random number generator initialized with seed r. Calculate $a = \rho(r) \oplus m$, $b = r \oplus H(a)$. Send $E(a||b)$.

Traitor tracing: $y = \Pi_{i=1}^{2k} {h_i}^{\delta_i}$. δ is the representation vector with respect to the base h. Convex combinations of representations are also solutions. Generate $l \geq 2k+2$ private keys with security parameter s to defend against coalition of size k. Choose g, a generator of G_q, r_i, $i = 1, 2, \ldots, 2k$ at random with $h_i = g^{r_i}$. Public key is $\langle y, h_1, h_2, \ldots, h_{2k} \rangle$ where $y = \Pi_{i=1}^{2k} {h_i}^{\alpha_i}$. Private key is θ_i with $\theta_i \gamma^{(i)}$ a representation of y. $\Gamma = \{\gamma^{(1)}, \gamma^{(2)}, \ldots, \gamma^{(l)}\}$ are public. Each $\gamma^{(i)} = \sum_j \gamma_j$ is a codeword. $\theta_i = \frac{\sum_{j=1}^{2k} r_j \alpha_j}{\sum_{j=1}^{2k} r_j \gamma_j}$. *Encrypt:* pick a randomly $C = \langle My^a, {h_1}^a, \ldots, (h_{2k})^a \rangle$. To decrypt $C = \langle C, H_1, \ldots, H_{2k} \rangle$, compute $M = \frac{S}{U^{\theta_i}}$ where

$U = \Pi_{i=1}^{2k} {H_i}^{\gamma_i}$. *Tracing:* Assume $q > max(l, 2k)$ examine $l - 2k - 1 \times 2k$ matrix A

$$A = \begin{pmatrix} 1 & 1 & 1 & ... & 1 \\ 1 & 2 & 3 & ... & l \\ 1^2 & 2^2 & 3^2 & ... & l^2 \\ ... & ... & ... & ... & ... \\ 1^{l-2k-1} & 2^{l-2k-1} & 3^{l-2k-1} & ... & l^{l-2k-1} \end{pmatrix}$$

Rowspace $\leftrightarrow$ polynomials of degree $\leq l - 2k - 1$. Let B be formed by the column vectors $b_1, b_2, \ldots, b_{2k}$, the basis of vectors satisfying $AX = 0(q)$. $\exists w$ of Hamming wt $\leq k$ with $vB = d$, null space of B $\leftrightarrow f$ with $deg(f) \leq l - 2k - 1$ and $v - w = \langle f(1), f(2), \ldots f(l) \rangle$ in all but (at most) k places. Use Berlekamp to find f from v.

3.4 Public Key Analysis

Define $L_n[u, v] = e^{vln(n)^u ln(ln(n))^{1-u}}$. $L_n[0, v]$ is polynomial and $L_n[1, v]$ is exponential. ECM is $L_n[\frac{1}{2}, 1 + o(1)]$. QS is $L_n[\frac{1}{2}, 1]$. NFS is $L_n[\frac{1}{3}, \frac{64}{9}^{1/3}]$. Probabilistic primality testing is polynomial.

Solovay-Strassen: Choose $1 \leq a \leq (n-1)$. If $(\frac{a}{n}) = a^{\frac{n-1}{2}} \pmod n$ then n is prime with probability $\frac{1}{2}$. Use the following to compute $(\frac{a}{n})$: (1) $(\frac{m_1 m_2}{n}) = (\frac{m_1}{n})(\frac{m_2}{n})$, (2) $(\frac{m}{n}) = -(\frac{n}{m})$, if $m = n = 1, 3 \pmod 4$, $(\frac{m}{n}) = (\frac{n}{m})$, otherwise, (3) $(\frac{2}{n}) = -1$, if $n = 1, 7 \pmod 8$, 1, if $n = 3, 5 \pmod 8$, (4) $(\frac{2^k t}{n}) = (\frac{2}{n})^k (\frac{t}{n})$.

Pockington: Let $n > 1$ and $s \mid (n-1)$. Suppose for some a, (1) $a^{\frac{n-1}{2}} = 1 \pmod n$, and (2) $\forall q, q|s$, $(a^{\frac{n-1}{q}} - 1, n) = 1$. Then $p \mid n$. So if $s > \sqrt{n}$, n is prime.

Pollard $p-1$: Extract prime factor p of n where $p-1$ is B smooth. $Q = \prod_{q|B} q^{\lfloor \frac{ln(n)}{ln(q)} \rfloor}$, where q is prime. Note $Q \mid p-1$. Now pick a, compute $gcd(a^Q - 1, n) = d$.

Pollard-ρ and Floyd: Let $x_{i+1} = f(x_i)$ with λ the length of the tail and μ the length of cycle. The *expected tail length* is $\sqrt{\frac{\pi n}{8}}$ and the *expected cycle length* is $\sqrt{\frac{\pi n}{2}}$. Floyd started at (x_0, x_0) and computes (x_i, x_{2i}) recursively from (x_{i-1}, x_{2i-2}). $x_m = x_{2m}$ for $\lambda < m < \lambda + \mu$.

Integer factoring with Pollard: $n = pq$. $f(x) = x^2 + 1 \pmod n$. Let $d = (x_{2m} - x_m, n)$. This should find p or q.

Solving discrete log problems: For the discrete log problem, $h = g^x \pmod n$. Let S_1, S_2, S_3 partition the multiplicative set $\mathbb{Z}_n^*$, $1 \notin S_2$ Define $x_{i+1} = f(x_i) = hx_i, x_i \in S_1$, $x_{i+1} = f(x_i) = x_i^2, x_i \in S_2$, and $x_{i+1} = f(x_i) = gx_i, x_i \in S_3$. Further, for a triple, (x_i, a_i, b_i), put $a_{i+1} = a_i \pmod n, x_i \in S_1$, $a_{i+1} = 2a_i \pmod n, x_i \in S_2$, and $a_{i+1} = a_i + 1 \pmod n, x_i \in S_3$; $b_{i+1} = b_i + 1 \pmod n, x_i \in S_1$, $b_{i+1} = 2b_i \pmod n, x_i \in S_2$, and $b_{i+1} = b_i \pmod n, x_i \in S_3$ and consider 3-tuples (x_i, a_i, b_i) with $(x_0, a_0, b_0) = (1, 0, 0)$. Then $log_g(x_i) = a_i + b_i log_g(h)$ is an invariant of the sequence. When $x_m = x_{2m}$, $a_m + xb_m = a_{2m} + xb_{2m}$ and $x = -\frac{a_{2m} - a_m}{b_{2m} - b_m} \pmod n$.

Quadratic Sieve: Want to find $x^2 = y^2 \pmod n$, then $(x - y, n)$ or $(x + y, n)$ is a factor of n. Factor base is $\mathcal{B}_B = \{-1, 2, 3, \ldots p_l\}, p_l \leq B$. Define a sequence $b_i = (\lfloor \sqrt{n} \rfloor + i)$, $a_i = b_i^2 - n = b_i^2 \pmod n$, $b_i^2 - a_i = n$. For the a_i's that factor over the base, find a bunch using linear algebra after taking the log. Then for these a_{i_l}'s, $\prod a_{i_l} = y^2 \pmod n$, where y is a product of the corresponding b_i's. Sieving finds $B-$smooth

elements of sequence. *Sieving:* Fix sieving interval $-C \le s \le C$, compute $f(s) = (s + \lfloor\sqrt{n}\rfloor)^2 - n$, find $s : p \mid f(s)$ - i.e.- find roots of $f(x) = 0 \pmod p$. For each p in the base, walk through sieving interval by steps of p for others. Divide each $f(s)$ in sieving interval by the highest possible dividing power of each p, ones with 1 or -1 remaining are smooth. Wiedemann algorithm for solving sparse linear equations is $L_n[\frac{1}{2}, 2v + o(1)]$. Sieving is $O(L_n[\frac{1}{2}, v + \frac{1}{4v} + o(1)]/p)$. *Reason:* Let $\psi(X, Y)$ be the number of $Y-$smooth numbers in $[1, X]$. $Pr(a \in [1, X]\ is\ Y - smooth) = \frac{\psi(X,Y)}{X}$; expected trials to find one: $\frac{X}{\psi(X,Y)}$ need about $\pi(Y)$ to get enough for a square and each takes $\pi(Y)$ work to test, so the total work is $W(X, Y) = \frac{\pi(Y)^2 X}{\psi(X,Y)}$. Minimum occurs when $Y = e^{\frac{1}{2}\sqrt{ln(X)ln(ln(X))}}$ and $X \approx n^{\frac{1}{2}+\epsilon}$. Try $n = 24961, 157$, for example.

Number Field Sieve: $F = \{p : p \le B\}$ want to find $a, \lambda : b = a + N\lambda$ and b is B-smooth so $\prod p \in F p^{a_p} = \prod_{p \in F} p^{b_p} \pmod N$. *Procedure:* (1) Fix λ, (2) let the array A have $A + 1$ 0's, (3) $\forall p \in F$, add $lg(p)$ to all positions congruent to $-\lambda N \pmod p$ and (4) choose a larger than some threshold. Construct two monics of degree d_1, d_2: $f_1(m) = f_2(m) = 0 \pmod N$ using the number fields $K_1 = \mathbb{Q}(\theta_1)$ and $K_2 = \mathbb{Q}(\theta_2)$. We have two homomorphisms $\phi_i : \mathbb{Z}[\theta_i] \to \mathbb{Z}/N\mathbb{Z}$, with $\theta_1 \mapsto m$. Set $S = \{(a, b) \in \mathbb{Z}^2 : (a, b) = 1\}$ satisfying $\prod_S (a - b\theta_1) = \beta^2$ and $\prod_S (a - b\theta_2) = \gamma^2$. Then $\phi_1(\beta)^2 = \phi_2(\gamma)^2 \pmod N$ and $(\phi_1(\beta) - \phi_2(\gamma)) \mid N$. What's left is to find S, β^2, f_1 and f_2. An algebraic integer is smooth if the the ideal it generates is divisible only by small primes. Define $F_i(X, Y) = Y^{d_i} f_i(X/Y)$ then $N_{\mathbb{Q}[\theta_i]/\mathbb{Q}}(a - bi) = F_i(a, b)$. Use two factor bases $\mathcal{F}_i = \{(p, \theta_i - r), f_i(r) = 0 \pmod p\}$. $F_i(a, b) = \prod_{(p_j, r) \in \mathcal{F}_i} {p_j}^{s_j^{(i)}}$. *Sieving:* (1) fix a, (2) init sieve array $-B \le b \le B$, $S[b] = lg(F_1(a, b) \cdot F_2(a, b))$, (3) $\forall (p, r) \in \mathcal{F}_i$ subtract $lg(p)$ from every element: $a - rb = 0 \pmod p$, (4) the desired b's are the ones: $S[b] \le Threshhold$. $\prod_{(a,b) \in S}(a - b\theta_i) = \mathcal{I}^2, \mathcal{I} \subseteq \mathbb{Z}[\theta_i]$. Now find enough relations such that $\prod_S (a - b\theta_1) = \beta^2$, etc.

Example: $N = 290^2 + 1$, $f_1(x) = x^2 + 1, f_2(x) = x - m, m = 290$. $f_1(m) = f_2(m) = 0 \pmod N$.

x	y	$N(x - iy)$	Factors	$x - my$	Factors
-38	-1	1445	$5 \cdot 17^2$	252	$2^2 \cdot 3^3 \cdot 7$
-22	-19	845	$5 \cdot 13^2$	5488	$2^4 \cdot 7^3$

$(-31 + i) = -(2 + i)(4 - i)^2$, $-22 + 19i) = -(2 + i)(3 - 2i)^2$, $(-38 + m)(-22 + 19m) = 2^6 3^2 7^4 = 1176^2 = (31 - 12i)^2$. $\phi_1(31 - 12i) = 31 - 12m = -3449$, $(-3449)^2 = (1176)^2$. $(N, -3449 + 1176) = 2273$, $(N, -3449 - 1176) = 37$.

Sieving analysis: Let $\psi(x, B)$ be the $B-$smooth numbers $\le x$. Let $\epsilon > 0$; if $x \ge 10$ and $w \le (ln(x))^{1-\epsilon}$, then $\psi(x, x^{\frac{1}{w}}) = xw^{-w+f(x,w)}$ and $\frac{f(x,w)}{w} \to 0$ for $w \to \infty$. Result: As $n \to \infty$, $\psi(n^a, L_n[u, v]) = n^a L_n[1 - u, -(\frac{a}{v})(1 - u)] + o(1)$. For *QS* $a \approx \frac{1}{2}$. *NFS* discrete log is $L_n[\frac{1}{3}, \frac{64}{9}^{\frac{1}{3}}]$. *MPQF:* $O(e^{(\sqrt{}ln(N)ln(ln(N)))})$. QS and NFS cross at 350 bits. Results below. Note: $1MIP - yr = 3.1 \times 10^{13}$ instructions. $120000Mip - years = 55Opteron - 2.2GHz - years$.

	RSA-129	RSA-130	RSA-200
Date	4/1996	8/1999	5/2005
Time (MIP-years)	500	8,000	120,000
Rows	3.5×10^6	6.7×10^6	6.4×10^7
Non Zero Members	1.4×10^8	4.2×10^8	1.1×10^{10}
NZ/R	39	62	171
Linear Algebra (hrs)	68	224	2160

RSA key	ECC key	Symmetric Key	ArithOps	SieveMem	LAMem
428	110	51	5.5×10^{17}	2GB	128MB
512	119	56	1.7×10^{19}	64MB	10GB
768	144	69	1.1×10^{23}	-	-
1024	163	79	1.3×10^{26}	256MB	100GB
2048	222	109	1.5×10^{35}	-	-

Finding discrete logs using Pohlig-Silver: Let g be a generator for F_q^*. Find x such that $g^x = y \pmod q$. $q-1 = {p_1}^{\alpha_1} \ldots {p_k}^{\alpha_k}$. First, precompute: $r_{i,j} = g^{\frac{j(q-1)}{p_i}}$, for $j = 1, 2, \ldots, p-1$. Want to find $x \pmod{p_i^{\alpha_i}}$, for each p_i then use Chinese Remainder Theorem (CRT). $x = x_0 + x_1 p + x_2 p^2 + \ldots + x_{\alpha-1} p^{\alpha-1}$. $y^{(q-1)/p} = g^{x(q-1)/p} = r_{p,x_0}$. This yields x_0. Next put $y_1 = \frac{y}{g^{x_0}}$. This reduces the discrete log over any group order to discrete log over p. This takes $O(\sum_{p||G|}(e(p)(lg(|G|) + \sqrt{p}))$ if we use Pollard.

Finding discrete logs using index calculus: Let g be a generator for F_q^* with $q = p^n$. Find x such that $g^x = y \pmod q$. *Precomputation phase:* Let $f(x)$ be an irreducible polynomial of degree n over F_p. Let B_m be the set of irreducible polynomials of degree $\leq m$. Pick random t and compute $c(x) = g(x)^t = c_0 \prod_{a(x) \in B_m} a(x)^{\alpha_{c,a}}$. $ind(c(x)) = ind(c_0) + \sum_{a(x) \in B_m} \alpha_{c,a} ind(a(x)) = t \pmod{q-1}$. Now solve for the $ind(a(x))$. *Solution phase:* To compute $ind(y(x))$, pick random t and compute $y(x)g(x)^t = \prod_{B_m} a(x)^{\alpha_{c,a}} \pmod{f(x)}$. This runs in $L_p[\frac{1}{2}, c+o(1)]$. In E_F, there is no good basis corresponding to primes.
Example: Let $q = p = 83$ and $g = 2$. $2^1 = 2 \pmod{83}$, so $ind_2(2) = 1$; $2^2 = 4 \pmod{83}$, so $ind_2(4) = 2$; $2^7 = 128 = 45 = 3^2 \cdot 5 \pmod{83}$, so $ind_2(45) = 7$; $2^{17} = 15 = 3 \cdot 5 \pmod{83}$, so $ind_2(15) = 7$. Rewrite the last two equations in log form as: $2ind_2(3) + ind_2(5) = 7 \pmod{82}$ and $ind_2(3) + ind_2(5) = 17 \pmod{82}$. Subtracting, we get $ind_2(3) = -10 = 72 \pmod{82}$. This is a simple example of solving the equations. Now suppose we want $ind_2(31)$. $31^2 = 48 = 2^4 3 \pmod{83}$, so $2ind_2(31) = 4ind_2(2) + ind_2(3) = 4 + 72 = 76 \pmod{82}$ and so $ind_2(31) = 38$. Sure enough, $(2^{17})^2) \cdot 2^4 = 59 \cdot 16 = 31 \pmod{83}$.

Shanks Baby/Giant: $\langle g \rangle = G$. Given $y = g^x$, find $x = log_g(y)$. Put $m = \sqrt{n}$, Compute (j, g^j) for $j = 1, \ldots, m$ sorted by second coordinate. Set $t \leftarrow g^{-m}$, $s \leftarrow y$.
For(i=0 to m-1) { /* is s second component?*/ if($s = g^j$) return($x = im + j$); $s \leftarrow st$}. Alternative: Solve $g^x = a \pmod p$. Pick $n : n^2 \geq (p-1)$ and compute $g^j \pmod p$ and $ag^{-nk} \pmod p$ for $0 \leq j, k \leq n$; match two lists giving $g^j = ag^{-nk} \pmod p$ or $g^{j+nk} = a \pmod p$.

Boneh-Joux attack on El Gamal/RSA with small messages and no preprocessing. Suppose we encrypt an m bit message M which is small then M is often smooth — i.e. $M = M_1 M_2$. If the El Gamal system is $\langle p, g, y = g^a \rangle$ and either the order of g is small (less than $\frac{p}{2^m}$) or $p - 1 = qs$ and the DL problem is tractable for subgroups of order s, much of the time ($\approx .18$) which solves the problem using about $2^{m/2}$ exponentiations. Here is the general problem: Let $z \in G_q \rightarrow \mathbb{Z}_p^*$, where G_q is a subgroup of order q; if $\Delta < 2^m$ and $u = z\Delta \pmod p$ then given u, find z. Here is a meet in the middle shortcut. Suppose $\Delta = \Delta_1 \Delta_2$, $\Delta_1 \leq 2^{m_1}, \Delta_2 \leq 2^{m_2}$, by tablizing Δ_1^q for possible Δ_1's and trying every possible Δ_2 in $(\frac{u}{\Delta_2})^q = \Delta_1^q (\mathrm{mod} p)$, we can find $\Delta = \Delta_1 \Delta_2$ in $O(2^{m_1} + 2^{m_2})$ time and 2^{m_1} space. With $m_1 = m_2 = 32$ this can solve for a 64 bit session key with probability about .18.

Defense for Boneh-Joux (OAEP or IND-CCA): $c = E(m) = f(a = M \oplus G(r) || b = r \oplus H(a)$
REACT: $E(m, r||s) : (a = f(x, r), b = k \oplus m, c = H(m, x, a, b)$, $k = G(x)$. For El Gamal: $a = Rand(1..q)$, $R = Rand(\langle g \rangle)$, $A = g^a$, $A' = Rg^a$, $k = G(R)$, $B = E_k(m)$, $C = H(R, m, A, a', B)$.

n	p	$H(B_n(p))$	n	p	$H(B_n(p))$
2	.5	2	3	.5	3
2	.60	1.94	3	.60	2.91
2	.75	1.62	3	.75	2.43
2	.80	1.44	3	.80	2.16
2	.90	.93	3	.90	1.4
2	.95	.57	3	.95	.85

λ	$H(P(\lambda))$	λ	$H(P(\lambda))$
.5	.91	.60	1.00
.75	1.14	.80	1.18
.90	1.27	.95	1.31

Shamir's attack on RSA with multiplication bug: Assume the RSA implementation uses the CRT (which yields a speedup of 4) and let the public key be $n = pq$ with $p < q$. Suppose that $a \times b$ (two 32 bit quantities) is computed incorrectly on a computer with a word size of w bits. We can pick $c = \lfloor \sqrt{n} \rfloor$ so $p < c < q$. Put $c = c_k 2^{wk} + c_{k-1} 2^{w(k-1)} + \ldots + c_1 2^w + c_0$ and select m such that $m = c_k 2^{wk} + c_{k-1} 2^{w(k-1)} + \ldots + a 2^w + b$. Assume we can have the flawed machine compute $m^d \pmod n$. Put $m_1 = m \pmod p$ and $m_2 = m \pmod q$. Since $p < m < q$ is likely, a and b are not likely to appear in the representation of m_1 but will appear in m_2. Thus $x_1 = {m_1}^d \pmod p$ will be computed correctly but $x_2 = {m_2}^d \pmod q$ will be computed incorrectly. Suppose $1 = up + vq$, the combined result will be computed as $y = m^d \pmod n = x_2 up + x_1 vq$. y will likely be correct $\pmod p$ but incorrect $\pmod q$. Thus $p \mid y^e - m$ but $q \nmid y^e - m$ and $p = (y^e - m, n)$. Padding interferes with this attack.

Weiner's attack: $|\alpha - \frac{p}{q}| \leq \frac{1}{2q^2}$ with $d < \frac{1}{3} N^{\frac{1}{4}}$. Put $N = pq$, $q < p < 2q, ed = 1 \pmod \phi$. $|\frac{e}{\phi} - \frac{k}{d}| < \frac{1}{d\phi}$ with $ed - k\phi = 1$, $|N - \phi| = |p + q + 1| < 3\sqrt{N}$ so $|\frac{e}{N} - \frac{k}{d}| \leq \frac{3k}{d\sqrt{N}} < \frac{1}{2d^2}$ and $\frac{k}{d}$ arises as a convergent, $\alpha = \frac{e}{N}$.

Coppersmith: Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial of $deg(f) = d$, $N \in \mathbb{Z}$. If $\exists x_0 : f(x_0) = 0 \pmod N$ with $|x_0| \leq X = N^{\frac{1}{d} - \epsilon}$, one can find x_0 in time polynomial in $lg(N)$ and $\frac{1}{\epsilon}$ for fixed d. This can be used to extend the *Franklin-Reiter* attack.

Observation: If $f(x) = f_0 + f_1 x + \ldots + f_d x^d$ and $\exists x_0 : f(x_0) = 0 \pmod n$ with $|x_0| < N^{\frac{1}{d}}$, find x_0 efficiently. The idea is to find $h(x) \in \mathbb{Z}[x]$ which shares a root with $f \pmod n$ with $||h||^2 = \sum_{i=0}^{deg(h)} |h_i|^2$ with $||h||$ small.

Lemma: Let $h(x) \in \mathbb{Z}[x]$, $deg(h) \leq n, X, N \in \mathbb{Z}^{>0}$; suppose $||h(XN)|| < \frac{N}{\sqrt{n}}$; if $|x_0| < X$ satisfies $h(x_0) = 0 \pmod N$ then $h(x_0) = 0$.

Suppose $f(x_0) = 0 \pmod n$ then $f(x_0)^k = 0 \pmod{N^k}$. For some m, set $g_{u,v}(x) = N^{m-v} x^u f(x)^v$, $0 \leq u < d, 0 \leq v \leq m$ then $g_{u,v}(x_0) = 0 \pmod{N^m}$. Fix m, try to find $a_{u,v} \in \mathbb{Z} : h(x) = \sum_{u \geq 0} \sum_{v=0}^{m} a_{u,v} g_{u,v}(x)$ that satisfies the lemma; that is $||h(xX)|| \leq \frac{N^m}{\sqrt{d(m+1)}}$ with $h(xX) = \sum_{u \geq 0} \sum_{v=0}^{m} a_{u,v} g_{u,v}(xX)$ that. Use LLL for this minimization problem. LLL conditions on $\langle b_1, b_2, \ldots, b_n \rangle$ are $\mu_{ij} = \frac{\langle b_i, b_i^* \rangle}{\langle b_i^*, b_i^* \rangle}$, $b_i^* = b_i - \sum_{j<i} \mu_{ij} b_j^*$, $||b_i^*||^2 \geq (\frac{3}{4} - \mu_{i,i-1}^2) ||b_{i-1}||^2$, if $x \in L, ||b_1|| \leq 2^{\frac{m-1}{2}} ||x||$, $||b_1|| \leq 2^{\frac{m}{4}} \Delta^{\frac{1}{m}}$.

Example: $f(x) = x^2 + ax + b$. Want to find $x_0 : f(x_0) = 0 \pmod N$. Set $m = 2$. $g_{00}(xX) = N^2$, $g_{10}(xX) = XN^2 x$, $g_{01}(xX) = bN + aXxN + XN^2 x$, $g_{11}(xX) = bNXx + aX^2 x^2 N + N^2 X^3 x^3$, $g_{02}(xX) = b^2 + 2abXx + (a^2 + 2b) X^2 x^2 + 2aX^3 x^3 + X^4 x^4$, $g_{12}(xX) = b^2 Xx + 2abX^2 x^2 + (a^2 + 2b) X^3 x^3 + 2aX^4 x^4 + X^5 x^4 5$.

$$A = \begin{pmatrix} N^2 & 0 & bN & 0 & b^2 & 0 \\ 0 & XN^2 & aXN & bNX & 2abX & Xb^2 \\ 0 & 0 & NX^2 & aNX^2 & (a^2+2b)X^2 & 2abX^2 \\ 0 & 0 & 0 & NX^3 & 2aNX^3 & (a^2+2b)X^3 \\ 0 & 0 & 0 & 0 & X^4 & 2aX^4 \\ 0 & 0 & 0 & 0 & 0 & X^5 \end{pmatrix}. \quad det(A) = N^6X^{15}, \ ||b_1|| < 2^{\frac{3}{2}}NX^{\frac{5}{2}}.$$

$b_1 = Au$, $Bu = (u_1, u_2, \ldots, u_6)$, $||h(xX)|| \leq \frac{N^2}{\sqrt{6}}$, $|x_0| \leq X = \frac{N^{\frac{2}{5}}}{48^{\frac{1}{8}}}$ and $|x_0| < N^{.39}$.

Common Modulus attack: Suppose $(e_1, e_2) = 1$ and m is encrypted both with an $\langle n, e_1\rangle$ scheme and a $\langle n, e_2\rangle$ scheme; let $c_1 = m^{e_1} \pmod n$ and $c_2 = m^{e_2} \pmod n$ with $d_1e_1 + d_2e_2 = 1$ then $m = {c_1}^{d_1}{c_2}^{d_2}$.

Small exponent attacks: Suppose $e = 3$ and $c_1 = {m_1}^e$, $c_2 = {m_2}^e$ with $m_2 = m_1 + \delta$, where δ is known. Put $F(x) = x^e - c_1 \pmod n$ and $G(x) = (x+\delta)^e - c_2 \pmod n$ then $(x-m) \mid (F(x), G(x))$ and we can recover m. Now if δ is unknown but $|\delta| < n^{\frac{1}{9}}$ and there is an algorithm, A (e.g.- Coppersmith's algorithm), that can find the roots, α of $f(x) = 0 \pmod n$ when $|\alpha| < n^{\frac{1}{9}}$, the foregoing attack can be extended. To do this, consider $F(x) = x^e - c_1 \pmod n$ and $G(x, y) = (x+y)^e - c_2 \pmod n$ and compute the resultant $h(y) = Res(F, G)$ in the ring $\mathbb{Z}_n[y]$; note h has a root, δ.

3.5 Lattice Methods

Lattices: $\Lambda = \mathbb{Z}\vec{b_1} + \mathbb{Z}\vec{b_2} + \ldots + \mathbb{Z}\vec{b_n}$ is the lattice generated by $\langle b_1, \ldots, b_n\rangle$. The volume of the fundamental region is $vol(\Lambda) = det(\vec{b_1}, \vec{b_2}, \ldots, \vec{b_n})$. If the basis vectors, $\langle b_1, \ldots, b_n\rangle$ are orthogonal, $vol(\Lambda) = ||b_1|| \cdot ||b_2|| \cdot \ldots \cdot ||b_n||$. The *orthogonal defect* of the basis $\langle b_1, \ldots, b_n\rangle$ is $\frac{||b_1|| \cdot ||b_2|| \cdot \ldots \cdot ||b_n||}{vol(\Lambda)}$.

Minkowski's Theorem: Let Λ be a lattice in $\mathbb{R}^n$ and $S \subseteq \mathbb{R}^n$ a convex, centrally symmetric region in $\mathbb{R}^n$. If $vol(S) > 2^n det(\lambda)$ then S has at least one non-zero lattice point of Λ.

Proof: Note that if $S_1 \cap S_2 = \emptyset$, $vol(S_1 \cup S_2) = vol(S_1) + vol(S_2)$. Let λ' be the lattice generated by $\langle e_1, e_2, \ldots, e_n$ and suppose $vol(S') > 2^n$. For $\vec{r} \in S'$, $\vec{r} = (\alpha_1 + x_1, \alpha_2 + x_2, \ldots, \alpha_n + x_n)$, where $\alpha_i \in \mathbb{Z}$ and $x_i \leq 1$, put $\vec{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ then define $T_{\vec{\alpha}}(r) = (x_1, x_2, \ldots, x_n)$. If $s \neq t \in S$ implies $T(r) \neq T(s)$ then $vol(S) = vol(T(S))$. $S = \bigcap_{\vec{a}lpha \in \mathbb{Z}^n} \vec{a}lpha + T(S)$. $vol(T_{\vec{0}}(S)) \leq 1$. So if $vol(\bigcap_\alpha T_{\vec{a}lpha}(S)) > 1$, S has two distinct non-zero points, r_1, r_2 such that $0 \neq r_1 - r_2 \in \mathbb{Z}^n$. Since S is centrally symmetric, $-r_1, -r_2 \in S$ also. If $vol(S') > 2^n$, there are at least $2^n + 1$ distinct points, $r_k \in S'$ with $r_i - r_j \in \mathbb{Z}^n$. So at least two of these points, say, r_j, r_k have the property that $r_j = r_k \pmod 2$. $0 \neq \frac{r_j - r_k}{2} \in \mathbb{Z}^n$ and $\frac{r_j - r_k}{2} \in S'$, by convexity. Now returning to S, let $\langle b_1, b_2, \ldots, b_n\rangle$ generate Λ and let $b_i = Ae_i$. $vol(\Lambda) = det(A)vol(e_1, e_2, \ldots, e_n)$, so if $vol(S) > 2^n vol(\Lambda)$, $\frac{vol(S)}{det(A)} > 2^n$. $S' = A^{-1}S$ is centrally symmetric, convex and generated by $\langle e_1, e_2, \ldots, e_n\rangle$; so, by the case above, there is a vector $0 \neq \alpha_1 e_1 + \alpha_2 e_2 + \ldots + \alpha_n e_n \in S'$. But then, $\alpha_1 b_1 + \alpha_2 b_2 + \ldots + \alpha_n b_n \in S$.

Shortest vector problems : The shortest vector problem, SVP, is : Given a lattice Λ, generated by $\langle b_1, \ldots, b_n\rangle$, find the vector $\vec{x} \in \Lambda$ with smallest length. SVP_γ is : Given a lattice Λ, generated by $\langle b_1, \ldots, b_n\rangle$, find a vector $\vec{x} \in \Lambda$ with $||v|| \leq \gamma\lambda$, where λ is the length of the shortest vector in Λ.

Theorem: If Λ is lattice generated by $b_1, b_2, \ldots, b_n$ and λ is the shortest vector in Λ, then $\lambda \leq \sqrt{n} det(\Lambda)^{\frac{1}{n}}$.

Proof: Let B_r be a ball centered at $\vec{0}$ with $r = \sqrt{n} det(\Lambda)^{\frac{1}{n}}$. $vol(B_r) > 2^n vol(\Lambda)$, so there is at least one non-zero vector, say x, in Λ inside B_r by Minkowski. Hence $\lambda \leq ||x|| \leq r$.

Hermite Normal Form: If A is an $m \times n$ dimensional matrix, there is a matrix $HNF(A)$ of the form

$$\begin{pmatrix} >0 & 0 & 0 & 0 & 0 & \dots & 0 \\ \geq 0 & >0 & 0 & 0 & 0 & \dots & 0 \\ \geq 0 & \geq 0 & >0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \geq 0 & \geq 0 & >0 & 0 & & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

. $HNF(A)$ is in normal form if (1) rightmost $m-n$ colums are 0, (2) $HNF(A)$ is lower triangular and, (3) all the elements in $HNF(A)$ are non-negative. Further, $HNF(A) = UA$, where U is unimodular.

Gram Schmidt orthogonalization algorithm (GSO): Given $\langle b_1, \dots, b_n \rangle$, compute an orthogonal basis $\langle b_1^*, \dots, b_n^* \rangle$ and μ_{ij} as follows:

1. $b_1^* = b_1$
2. for $i = 2$, $i \leq n$
   2.1. $b_i^* \leftarrow b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*, \mu_{ij} = \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)}$
3. return $\langle b_1^*, \dots, b_n^* \rangle$ and μ_{ij}

Generally, $\langle b_1^*, \dots, b_n^* \rangle \notin \Lambda$. The basis reduction algorithm finds a new reduced basis $\langle b_1, \dots, b_n \rangle$ from the original basis and the output of the Gram-Schmidt orthogonalization algorithm.

Size reduction algorithm (SRA): Given $\langle b_1, \dots, b_n \rangle$, produce reduced basis $\langle b_1, \dots, b_n \rangle$ GSO vectors $\langle b_1^*, \dots, b_n^* \rangle$ and GSO coefficients μ_{ij}.

1. Run GSO to get $\langle b_1^*, \dots, b_n^* \rangle$ and μ_{ij}.
2. for $i = 2$ up to n
   2.1. for $j = (i-1)$ downto 1
      2.1.1. $b_i \leftarrow b_i - \lfloor \mu_{ij} \rceil b_j$
      2.1.2. for $k = 1$ to j
         2.1.2.1. $\mu_{ik} \leftarrow \mu_{ik} - \lfloor \mu_{ij} \rceil \mu_{jk}$
3. return $\langle b_1, \dots, b_n \rangle$, $\langle b_1^*, \dots, b_n^* \rangle$, μ_{ij}

LLL motivation: $AU = B$ has a solution iff $M = \begin{pmatrix} I & 0 \\ A & -B \end{pmatrix}$ and $M[U,1]^T = [U,0]^T$ has a solution with U a $0,1$ vector. Since $||[U,0]^T|| \leq n$, a short vector in the lattice generated by the column space of M is likely to be close to a solution of $AU = B$. Let L be a lattice generated by M, $vol(L) = |det(M)|$ Not all lattices are generated by linearly independent vectors; for example $\langle (1,2), (1,1), (2,1) \rangle$.

Lattices in 2 dimensions (vectors are columns) $[a,b]$ is reduced iff $||a|| \leq ||b||$ and $||a||, ||b|| \leq ||a+b||, ||a-b||$. Lemma: If $||x|| \leq ||x+y||$ then $||x+y|| \leq ||x+\alpha y||$, $\alpha > 1$. Let $\lambda_k = min_x |\{v \in \mathcal{L}(B) - \{0\} : ||v|| \leq x\}| \geq k$ (so λ_1 is the shortest vector in the lattice.) Theorem: If a, b is a basis, $||a|| = \lambda_1$, $||b|| = \lambda_2$

iff $[a, b]$ is a reduced basis. Gauss algorithm: (1) Find μ: $||b - \mu a||$ is minimal. (2) if $||a - b|| > ||a + b||$ replace b with $-b$. (3) if $[a, b]$ is not reduced, swap a and b and go to 1. Note: LLL Gives an approximation to reduced basis $n > 2$.

Definitions: $\langle b_1, b_2, \ldots b_n\rangle$ is *size reduced* if $|\mu_{ij}| \leq \frac{1}{2}$. $\langle b_1, b_2, \ldots, b_n\rangle$ is *LLL reduced* with respect to δ if

1. $\langle b_1, b_2, \ldots, b_n\rangle$ is size reduced.
2. $\delta||b_i^*||^2 \leq ||b_{i+1}^*||^2 + \mu_{i+1,i}^2||b_i^*||^2$.

LLL algorithm: Input is basis $\langle b_1, \ldots, b_n\rangle$. Output is LLL reduced basis.

1. Run SRA to get reduced $\langle b_1, \ldots, b_n\rangle$, $\langle b_1^*, \ldots, b_n^*\rangle$, μ_{ij}
2. Compute $B_i = ||b_i^*||^2$
3. for $i = 2$ to $n - 1$
   - 3.1. if $(\delta - \mu_{i+1,i}^2)B_i > B_{i+1}$
     - 3.1.1. swap b_i and b_{i+1}
     - 3.1.2. start again at step 1
4. return $\langle b_1, \ldots, b_n\rangle$

LLL Theorem: Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice with an LLL reduced basis $\langle b_1, b_2, \ldots, b_n\rangle$ and let λ be the length of the shortest vector in Λ. Then

1. $||b_1|| \leq 2^{\frac{n-1}{2}} vol(\Lambda)^{\frac{1}{n}}$
2. $||b_1|| \leq 2^{\frac{n-1}{2}}\lambda$
3. $||b_1|| \cdot ||b_2|| \cdot \ldots \cdot ||b_n|| \leq 2^{\frac{n(n-1)}{4}}$

Theorem: Let Λ be a lattice with basis $\langle b_1, \ldots, b_n\rangle$ with $||b_i|| < X$ for all i. Let $\frac{1}{4} < \delta < 1$. Then LLL's running time is $O(n^6 lg(X)^3)$.

Theorem: Let $\langle b_1, b_2, \ldots, b_n\rangle$ be a LLL-reduced basis for Λ with $\delta = \frac{3}{4}$ and $\langle b_1^*, \ldots, b_n^*\rangle$ as above and $B_i = ||b_i^*||^2$. Then

1. $B_i \leq 2B_{i+1}$
2. $B_i \leq ||b_i||^2 \leq (\frac{1}{2} + 2^{i-2})B_i$
3. $||b_j|| \leq 2^{\frac{i-1}{2}}||b_i^*||$
4. $\lambda(\Lambda) \geq min_i||b_i^*||$

Proof: Since the basis is reduced, $\mu_{i+1,i}^2 \leq \frac{1}{4}$. The LLL condition with $\delta = \frac{3}{4}$ gives 1. GSO insures $b_i = b_i^* + \sum_{j=1}^{i-1} \mu_{ij} b_j^*$ and by orthogonality, $||b_i^*|| \leq ||b_i||$ and $||b_i||^2 = B_i + \sum_{j=1}^{i-1} \mu_{ij}^2 B_j$. $\mu_{ij}^2 B_j \leq \frac{1}{4}B_j \leq \frac{1}{4}2^{i-j}B_i$ giving 2, since $||b_i||^2 \leq B_i(1 + \frac{1}{4}\sum_{j=1}^{i-1} 2^{i-j}) = B_i(1 + \frac{1}{4}(2^i - 2)) = B_i(\frac{1}{2} + 2^{i-2})$. For $j \geq 1$, $\frac{1}{2} + 2^{j-2} \leq 2^{j-1}$, so 2 implies $||b_j||^2 \leq 2^{j-1}B_j$. Since $B_j \leq 2^{i-j}B_i$, by 1, we get $||b_j||^2 \leq 2^{j-1}2^{i-j}B_i = 2^{i-1}B_i$. We get 3 by taking square roots. If $\vec{v}$ is the shortest vector, $\vec{v} = \sum_{i=1}^{n} x_i b_i, x_i \in \mathbb{Z}$, we get $\vec{v} = \sum_{i=1}^{n}(x_i b_i^* + \sum_{j=1}^{i-1}(x_i \mu_{ij} b_j^*)) = \sum_{i=1}^{n}(x_i + \mu_{i+1,i}x_{i+1} + \ldots + \mu_{ni}x_n)b_i^*$. Let i be the largest index with $x_i \neq 0$. The last equation and orthogonality give $||\vec{v}|| \geq |x_i|||b_i^*||$ which gives 4.

Theorem: Let $\langle b_1, b_2, \ldots, b_n \rangle$ be a LLL-reduced basis for Λ with $\delta = \frac{3}{4}$ then

1. $||b_1|| \leq 2^{\frac{n-1}{2}} \lambda$
2. $vol(\Lambda) \leq \prod_{i=1}^{n} ||b_i|| \leq 2^{\frac{n(n-1)}{4}} vol(\Lambda)$
3. $||b_1|| \leq 2^{\frac{n-1}{4}} vol(\Lambda)^{\frac{1}{n}}$

   Proof: By the previous proposition $||b_i^*||^2 \geq 2^{\frac{1-i}{2}} ||b_1^*||$, But $b_1 = b_1^*$, so $\lambda \geq min_i ||b_i^*|| = 2^{\frac{1-n}{2}} ||b_1||$. $vol(\Lambda) = \prod_{i=1}^{n} ||b_i^*||$ and inequality 2 follows from $||b_i^*|| \leq ||b_i||$ and part 3 of the proposition. $||b_1|| \leq 2^{\frac{i-1}{2}} ||b_1^*||$ now gives $||b_1||^n \leq \prod_{i=1}^{n} 2^{\frac{i-1}{2}} ||b_i^*|| = 2^{\frac{n(n-1)}{4}} vol(\Lambda)$.

Theorem: K is *convex* and *symmetric* iff $x, y \in K$ implies $ax + by \in K$ provided $|a| + |b| \leq 1$.

Minkowski: Let L be a lattice of rank r. Let v_1 be the shortest vector, v_i the shortest vector independent of $\langle v_1, \ldots, v_{i-1} \rangle$, then $|v_1||v_2| \ldots |v_r| \leq \frac{2^r}{vol(B_r)} d(L)$ where $vol(B_r) = \frac{\pi^{\frac{r}{2}}}{\Gamma(1+\frac{r}{2}))}$.

Minkowski's theorem on linear forms: Let $\Lambda \in \mathbb{R}^N$ and $L_1, \ldots, L_N$ be linear forms with associated matrix C; if $det(C) d(\lambda) \leq \epsilon_1 \epsilon_2 \ldots \epsilon_N$, there is a lattice point $\lambda \neq 0$ such that $|L_m(\lambda)| \leq \epsilon_m$. Corollary: $\exists l : L_m(l) \leq (det(C))^{\frac{1}{N}}$.

Low density subset sum. $\sum a_i s_i = s$ look at matrix formed by I_n with bottom row $(\frac{1}{2}, \ldots, \frac{1}{2}, ms)$ and first n entries in rightmost columns $(ma_1, ma_2, \ldots, ma_n)$. Now round.

Weakness due to partial knowledge: If $n = pq$ has m bits and we know the first or last $\frac{m}{4}$ bits of p, then n is easy to factor. If plaintext is short, match $cx^{-e} = y^e$ to get $c = (xy)^e \pmod{n}$. If $q < p < 2q$ and $1 \leq d, e < \psi(n)$ with $de = 1 \pmod{\psi(n)}$ and $d < \frac{1}{3} n^{\frac{1}{4}}$ then d can be found easily.

Attack on RSA using LLL: Suppose message is of the form "M xxx" where only 'xxx' varies (e.g.- "The key is xxx"). Thus the message is of the form $B + x$ where B is fixed and $|x| < Y$. $c = (B + x)^3 \pmod{n}$ and $f(T) = (B + T)^3 - c = T^3 + a_2 T^2 + a_1 T + a_0 \pmod{n}$. We want to find $x : f(x) = 0 \pmod{n}$. Let $v_1 = (n, 0, 0, 0)$, $v_2 = (0, Yn, 0, 0)$, $v_3 = (0, 0, Y^2 n, 0)$, $v_4 = (a_0, a_1 Y, a_2 Y^2, Y^3)$. Then $||b_1|| \leq 2^{\frac{3}{4}} |det(v_1, v_2, v_3, v_4)| = 2^{\frac{3}{4}} n^{\frac{3}{4}} Y^{\frac{3}{2}}$. $b_1 = c_1 v_1 + \ldots + c_4 v_4 = (e_0, Y e_1, Y^2 e_2, Y^3 e_3)$; $e_0 = c_1 n + c_4 a_0$, $e_1 = c_2 n + c_4 a_1$, $e_2 = c_3 n + c_4 a_2$, $e_3 = c_4$, and $g(T) = e_3 T^3 + e_2 T^2 + e_1 T + e_0$. Since $f(x) = 0 \pmod{n}$ and $c_4 f(T) = g(T) \pmod{n}$, $0 = c_4 f(x) = g(x) \pmod{n}$. If $Y < 2^{\frac{7}{6}} n^{\frac{1}{6}}$, $|g(x)| \leq 2||b_1||$ (use C-S) but $||b_1|| \leq 2^{-1} n$ so $|g(x)| < n$ and $g(x) = 0$ yielding 3 candidates for x. *Coppersmith* extended this to small solutions of polynomials of degree d using a $d + 1$ dimensional lattice by examining the monic polynomial $f(T) = 0 \pmod{n}$ of degree d when $|x| \leq n^{\frac{1}{d}}$.

GGH public key scheme: Let $n \in \mathbb{N}$ be the security parameter. $M \in \mathbb{Z}$ and $\sigma = 3$.

1. $\mathcal{M} = \{-M, \ldots, 0, 1, \ldots M\}$ is the message space $\mathcal{C} = \mathbb{Z}^n$ is the cipherspace.
2. For key generation, choose $B \in \mathbb{Z}^{n \times n}$ uniformly over small integers (say between -4 and 4). Check that B is invertible. B is the private key. Let H be the HNF of B. H is the public key.
3. To encrypt, $\vec{m} \in \{-M \ldots 0, 1, \ldots M\}$, choose random noise vector, $\vec{r} \in \{-\sigma, \sigma\}^n$. $\vec{c} = H\vec{m} + r$.
4. To decrypt, $\vec{m} = H^{-1} B \lfloor B^{-1} \vec{c} \rceil$ ($\lfloor B^{-1} \vec{c} \rceil$ is called the Babai rounding of $\vec{c}$ with respect to B).

NTRU public key scheme: $R = \mathbb{Z}[x]/(x^N - 1)$. Define $\mathcal{T}(d_1, d_2)$ are ternary polynomials n R with d_1 coefficients 1, d_2 coefficients equal to -1 and the rest 0. Let p be prime and make sure $(N, p) = (N, q) = 1$ and $q > (6d + 1)p$. $R_p = \mathbb{Z}_p[x]/(x^N - 1)$, $R_q = \mathbb{Z}_q[x]/(x^N - 1)$.

1. $\mathcal{M} = R_p$ and $\mathcal{C} = R_q$.
2. For key generation, pick two polynomials $f, g \in R$ with $f \in \mathcal{T}(d + 1, d)$ and $g \in \mathcal{T}(d, d)$. Check that f is invertible $(\text{mod } q)$ and $(\text{mod } p)$, so $f_p \cdot f = 1 \,(\text{mod } p)$ and $f_q \cdot f = 1 \,(\text{mod } q)$. Put $h = f_q \cdot g \,(\text{mod } q)$. Public key is (N, p, q, h), the private key is f.
3. To encrypt, encode the message in a polynomial, of degree $< N$, with coefficients, $-\frac{p-1}{2} \leq m_i \leq \frac{p-1}{2}$. Choose $r \in \mathcal{T}(d, d)$. $c = prh + m \,(\text{mod } q)$.
4. To decrypt, compute $a = fc \,(\text{mod } q)$ and represent a with integer coefficients between $-\frac{p-1}{2}$ and $\frac{p-1}{2}$. $m = f_p a \,(\text{mod } p)$. To verify, check $a = fc = f(prh + m) \,(\text{mod } q) = prg + fm \,(\text{mod } q)$. The largest coefficient of this is at most $p \cdot 2d + (2d + 1)\frac{p}{2}$ and since $q > (6d + 1)p$ the coefficients have magnitude less than $\frac{q}{2}$.

For a polynomial, $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}$, we can define the circulant matrix, C_f, whose top roq consists of the coefficients, in order. On each successive row, the entries shift on place left. If $g(x) = b_0 + b_1 x + \ldots + b_{N-1} x^{N-1}$, $(b_0, b_1, \ldots, b_{N-1})C_f = \tilde{f}\tilde{g}$ is the convolution. NTRU in the lattice context is as follows. $\tilde{f} C_h = \tilde{g} \,(\text{mod } q)$. The matrix

$$A = \begin{pmatrix} I_N & C_h \\ 0 & qI_N \end{pmatrix}$$

generates a lattice. A short vector in this lattice is $(\tilde{f}, \tilde{g})$.

Learning with Errors (LWE): If $a_i \in \mathbb{Z}_q^n$ are chosen uniformly at random. $s \in \mathbb{Z}_q^n$ is secret and we are given $m \geq n$ approximate equations $a_1 \cdot s = b_1$, $a_2 \cdot s = b_2$, $\ldots a_m \cdot s = b_m$. The errors, $e_1, e_2, \ldots, e_m$ are small and chosed from χ. We often use the discrete Gaussian for χ: $p(x) = \frac{1}{c} e^{\frac{x^2}{2\sigma^2}}, x \in \mathbb{Z}$, where $c = \sum_{k \in \mathbb{Z}} e^{\frac{k^2}{2\sigma^2}} \approx \sigma\sqrt{2\pi}$. Parameter width is $s = \frac{s}{\sqrt{2\pi}}$.

Definition: Let $n, m, q \in \mathbb{N}, m \geq n, q \geq 2$ with $s \in \mathbb{Z}_q^n$. Let $A \in \mathbb{Z}_q^{m \times n}$ with entries choosen uniformly at random. Let $e \in \mathbb{Z}_q^m$ be drawn from χ^m. The *search LWE* problem is to find s, given A and $b = As + e$. The *decision LWE* problem is to distinguish between (1) $b = As + e$ and (2) a uniform distribution.

Piekert showed with the right parameters, breaking the cipher is equivalent to worst case LWE.

Regev: Let $n \in \mathcal{N}$ and $m, q \in \mathcal{N}$ are polynomial in n. $\chi = D_{\mathcal{Z},s}$, $s > \alpha q > 2\sqrt{n}$ and $0 < \alpha < 1$. LWE is as hard as worst case $SIVP_\gamma$, $\gamma = O(\frac{n}{\alpha})$.

LWE Public scheme: $m, n, q \in \mathbb{N}$, $m \geq n, q \geq 2$, χ and error distribution on $\mathbb{Z}$. l is plaintext length. $\mathcal{M} = \{0, 1\}^l$, $\mathcal{C} = \mathbb{Z}_q^n \times \mathbb{Z}_q^l$.

1. Keys: Choose $S \in \mathbb{Z}^{n \times l}$ and $A \in \mathbb{Z}^{m \times n}$ uniformly at random and choose $E \in \mathbb{Z}^{m \times l}$ according to χ. Public key is $(A, P = AS + e)$. Secret key is S.
2. to encrypt $v \in \{0, 1\}^l$, choose $a \in \{0, 1\}^m$ uniformly at random. Cipher is $(u, c) = (A^T a, P^T a + \lfloor \frac{q}{2} \rceil v)$.
3. To decrypt, $D = \lfloor \lfloor \frac{q}{2} \rceil^{-1} (c - S^T u) \rceil \,(\text{mod } 2)$.

A decryption error occurs if the magnitude of a coordinate of $E^T a$ is greater than or equal to $\frac{q}{4}$. If χ is the discrete gaussian, the coordinates of $E^T a \leq \sqrt{ms}$ with high probability. Again, considering a lattice generated by $AS + e$, if we can fins a short vector, we can identify S.

To convert LWE to a lattice problem, let $\vec{s}$ is a column of S and $\vec{e}, \vec{b}$ be the corresponding vectors of E and P, respectively in $\Lambda_q(A^T)$. This is a closest vector problem. To embed it in the shortest vevctor problem, Let $H \in \mathcal{Z}_1^{m \times m}$ where the columns of H form a basis for $\mathcal{Z}_q^m$. Pick $M > 0$. Consider

$$B = \begin{pmatrix} H & b \\ 0 & M \end{pmatrix}.$$

Linear combinations of columns of H give a short vector $e' = (e, M)^T$. Choosing M properly gives e with high probability.

Ring learning with errors (RLWE): LWE keys are large. For ring LWE, use $R = \mathbb{Z}_q[x]/(x^n + 1)$, where n is a power of 2. A, s, e are replaced by elements of R. The ring-LWE problem is to find $s \in R$ given $a \in R$ and $b = as + e \in R$, again e is small according to the error distribution. There is a reduction from worst case SVP_γ to R-LWE.

LLL example: $\delta = \frac{3}{4}$, $b_1 = (2, 3, 14)^T$, $b_2 = (0, 7, 11)^T$, $b_3 = (0, 0, 23)^T$. LLL-reduced basis is $b_1 = (-2, 4, -3)^T$, $b_2 = (-4, 2, 6)^T$, $b_3 = (4, 6, 5)^T$.

GGH example: $m = (4, -4, 1, 3)^T$. $r = (-1, 1, 1, -1)^T$. $B = \begin{pmatrix} 2 & -3 & 1 & -4 \\ -1 & 1 & 0 & 4 \\ -1 & 3 & 2 & 1 \\ -1 & -4 & 3 & -3 \end{pmatrix}$. $H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 44 & 18 & 4 & 45 \end{pmatrix}$.
$c = Hm + r = (2, 03, 2, 210)^T$. $B^{-1} = \frac{1}{49} \begin{pmatrix} 61 & 45 & 10 & -27 \\ -10 & -13 & 8 & -2 \\ 29 & 23 & 16 & -4 \\ 33 & 38 & 3 & -13 \end{pmatrix}$. $H^{-1} = \frac{1}{49} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$.

GGH example: $m = (4, -4, 1, 3)^T$. $r = (-1, 1, 1, -1)^T$. $B = \begin{pmatrix} 2 & -3 & 1 & -4 \\ -1 & 1 & 0 & 4 \\ -1 & 3 & 2 & 1 \\ -1 & -4 & 3 & -3 \end{pmatrix}$. $H = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 44 & 18 & 4 & 45 \end{pmatrix}$.
$c = Hm + r = (2, 03, 2, 210)^T$. $B^{-1} = \frac{1}{49} \begin{pmatrix} 61 & 45 & 10 & -27 \\ -10 & -13 & 8 & -2 \\ 29 & 23 & 16 & -4 \\ 33 & 38 & 3 & -13 \end{pmatrix}$. $H^{-1} = \frac{1}{49} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{-44}{15} & \frac{-18}{49} & \frac{-4}{49} & \frac{1}{49} \end{pmatrix}$.

LWE example: $n = 4$, $q = 23$, $m = 8$, $\alpha = \frac{5}{23}$, $\sigma = \frac{s}{\sqrt{2\pi}}$, $s = 5$. $A = \begin{pmatrix} 9 & 5 & 11 & 13 \\ 0 & 22 & 22 & 22 \\ 6 & 21 & 17 & 18 \\ 22 & 22 & 22 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 1 & 22 & 1 & 22 \\ 22 & 0 & 0 & 1 \end{pmatrix}$.

$S = \begin{pmatrix} 5 & 2 & 9 & 1 \\ 6 & 8 & 19 & 1 \\ 19 & 18 & 9 & 18 \\ 9 & 2 & 14 & 18 \end{pmatrix}$. $E = \begin{pmatrix} 0 & 22 & 1 & 21 \\ 0 & 22 & 22 & 22 \\ 6 & 21 & 17 & 18 \\ 22 & 22 & 22 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 \\ 1 & 22 & 1 & 22 \\ 22 & 0 & 0 & 1 \end{pmatrix}$. $P = \begin{pmatrix} 10 & 5 & 21 & 7 \\ 3 & 1 & 13 & 1 \\ 19 & 15 & 6 & 13 \\ 22 & 22 & 22 & 0 \\ 9 & 20 & 20 & 17 \\ 15 & 21 & 1 & 2 \\ 0 & 12 & 3 & 19 \\ 16 & 2 & 7 & 15 \end{pmatrix}$. $v = (1, 0, 1, 1)^T$, $a = (1, 1, 0, 1, 0, 0, 1)^T$. $\lfloor \frac{23}{2} v \rceil = (12, 0, 12, 12)^T$, $(u, c) = ((3, 14, 2, 7)^T, (14, 5, 7, 5)^T)$. $m' = c = S^T u \pmod{23} = (11, 21, 12, 10)^T$. $\lfloor \frac{23}{2} v = (12, 0, 12, 12)^T$. Recover $(1, 0, 1, 1)^T$.

NTRU example: $N = 5$, $p = 3$, $q = 29$, $d = 1$, $f = x^4 + x^3 - 1$, $g = x^3 - x$. $m = x^3 + x$. $f_p = x^3 - x^2 + x - 1$, $f_q = -5x^4 + 8x^3 - 3x^2 + 11x + 15$. $h = f_q g = 8x^4 + 21x^3 + 25x^2 + 20x + 15 \pmod{29}$. $c = prh + fm \pmod{29} = 8x^4 + 21x^3 + 25x^2 + 20x + 15$. $a = fc \pmod{29} = -2x^4 + 2x^3 + 4x^2 - 3x + 1$. $m = x^3 + x$.

NIST contestants: The contestants use the following security parameters:

1. New hope uses ring LWE with parameters $q = 12289$, $n = 1024$.
2. Frodo uses LWE onunstructures lattices with $m = n = 1344$, $q = 2^{16}$, $\sigma = 1.4$, $-6 \leq x \leq 6$, for AES-256 parity. Cipher text size is 21644-bytes. Decoding error rate is 2^{-252}. The public key size is about 1 Mb.
3. The NTRU parameters are $n = 1024$ $N = 743$, $q = 2048$, $d_1 = 11$, $d_2 = 11$ giving 256-bit security. Public key size about 2 KB.
4. McElice uses $n = 6960$, $k = 5413$, $t = 119$ with a Goppa code. The key size is 8MB.

3.6 Symmetric Key Analysis

DES S Box Criteria: (1) S is not linear or affine in the inputs, (2) changing 1 bit of input changes at least 2 bits of output, (3) minimize differences between 1s and 0s if one input bit is held constant, (4)$Ham(S(x) \oplus S(x \oplus 001100)) > 1$, and (5) $S(x) \neq S(x \oplus 11ab00)$.

Differential cryptanalysis: Notation: $x \to y, p$ means input difference x produces output y with probability p. If $x' \to y'$ and $D_j(x', y') = \{u : S_j(u) \oplus S_j(u \oplus x') = y'\}$ then $x \oplus k \in D_j(x', y')$, and $k \in D_j(x', y') \oplus x$. Set $\tau_j(x, x', y') = \{k : k \in D_j(x', y') \oplus x\}$ and $test_j(E_j, {E_j}^*, C'_j) = \tau_j(E_j, E_j \oplus E_j^*, C'_j)$. Note: some candidate keys will scritch. To convert from chosen to known attack, select $2^{32}\sqrt{2m}$ pairs, about m of these will have the right difference x produces output y with probability p. If $x' \to y'$ and $D_j(x', y') = \{u : S_j(u) \oplus S_j(u \oplus x') = y'\}$ then $x \oplus k \in D_j(x', y')$, and $k \in D_j(x', y') \oplus x$. Set $\tau_j(x, x', y') = \{k : k \in D_j(x', y') \oplus x\}$ and $test_j(E_j, {E_j}^*, C'_j) = \tau_j(E_j, E_j \oplus E_j^*, C'_j)$.

3-round attack: (L_0, R_0), $R_3 = L_2 \oplus f(R_2, k_3) = L_0 \oplus f(R_0, k_1) \oplus f(R_2, k_3)$. Choose ${R_0}' = 000000$, so that $f(R_0, k_1) \oplus f(R_0^*, k_1) = 0$, get $R'_3 = L'_0 \oplus f(R_2, k_3) \oplus f(R_2^*, k_3)$. Set $C' = P^{-1}(R'_3 \oplus L'_0)$ which is the output xor for round 3. Compute $E = E(L_3)$, $E^* = E(L_3^*)$. Calculate $test_j(E_j, {E_j}^*, C'_j)$, for $j = 1, 2, ..., 8$ after choosing plaintexts. Can do this since $R_2 = L_3$ is known. Note that key bits overlap on initial and final rounds and must satisfy both conditions.

Cost of differential cryptanalysis: The *signal to noise ratio*, S/N ratio, is the ratio of the count in the correct key bin to the average count in a key bin. For the differential attack to succeed, $S/N > 1$. Assume there are m pairs of chosen text, p is probability of characteristic, k is the number of key bins (number of possible keys), γ is number of suggested keys per pair. There are about mp right pairs (and the right key is always counted). If λ is the ratio of non-discarded pairs to the number pairs, then the average count is $\frac{\gamma\lambda m}{k}$ and so $S/N = \frac{pk}{\gamma\lambda}$. Note that differential differs from the product of round differential characteristics (which is what we used); the differential probability considers all valid pairs with correct first and final round differentials combine (add) to provide the differential probability estimate. Usually, however, the product of probabilities of the round characteristics is a good estimate for the differential, if not, other attacks, like related key attacks, often work.

6-round attack: Use $(L'_0, R'_0) = (0x40080000, 0x04000000)$, $(L'_1, R'_1) = (0x04000000, 0x00000000)$, $p = .25$; $(L'_2, R'_2) = (0x00000000, 0x04000000)$, $p = 1$; $(L'_3, R'_3) = (0x04000000, 0x40080000)$, $p = .25$. $L_6 = L_5 \oplus f(R_5, K_6)$, $R_4 = L_3 \oplus f(R_3, K_4)$, and $L_5 = R_4$ so $L'_3 \oplus L'_6 = f(R_3, K_4) \oplus f(R_5, K_6) \oplus f(R^*_3, K_4) \oplus f(R^*_5, K_6)$. Estimate $L'_3 = 0x04000000$ and $R'_3 = 0x40080000$ with $p = \frac{1}{16}$. Use this to estimate input xor for S-boxes of round 4. Get $C'_1C'_2...C'_8 = P^{-1}(L'_6 \oplus 0x04000000)$ and $E'_1E'_2...E'_8 = E(R_5)$. $f(K_6, R_5) \oplus f(K_6, R^*_5) = 0$ since xors to $S2, S5, S6, S7, S8$ are 0 so $f(K_4, R_3) \oplus f(K_4, R^*_3) = P^{-1}(L'_6 \oplus 0x04000000)$. Right pairs bump count for correct key bits, wrong pairs are random. *Filter:* If $|test_j(E_j, {E_j}^*, C'_j)| = 0$, for all $j = 2, 5, 6, 7, 8$, this is a wrong pair; the probability that a wrong pair satisfies this at random is $(\frac{4}{5})^5 = \frac{1}{3}$ since only $\frac{4}{5}$ of the differentials are possible in each S-box. $\frac{2}{3}$ of the wrong pairs are detected this way, so ratio of right pairs ("RP") remaining is $\frac{\frac{1}{16}}{\frac{1}{16}+\frac{15}{16}\times\frac{1}{3}} = \frac{1}{6}$. Number of suggested pairs is $\Pi|test_j(E_j, {E_j}^*, C'_j)|$, for $j = 2, 5, 6, 7, 8$, correct values will be suggested $\frac{3n}{16}$ times; incorrect strings at random among approximately 2^{30} values. Let T_j be the counter vector of length 64. For each pair compute T^i_j, $j = 2, 5, 6, 7, 8$, $1 \le i \le n$. For $I \subseteq \{1, 2, \ldots n\}$, $\sum_{i \in I} T^i_j$. There should be some I of size about $\frac{3n}{16}$, this is the suggested key. Here n is the number of pairs and all of the remaining indexes have 1 in the vector.

Another 3-round Characteristic: L'_0, R'_0: 0x00200008, 0x00000400, L'_1, R'_1: 0x00000400, 0x00000000, $p = .25$; L'_2, R'_2: 0x00000000, 0x00000400, $p = 1$; L'_3, R'_3: 0x00000400, 0x00200008, $p = .25$. **Iterative Characteristic:** $\Omega_P = (19600000|00000000), p = \frac{1}{234}$. These can be concatinated.

5-round differential and 0R, 1R, 2R attacks: The differential is $\Omega_P = (400046D0||02000000) = \Omega_T$ consisting of $02000000 \to 40004010, p_1 = \frac{14}{64}$, $000006c0 \to 02000000, p_2 = \frac{12 \cdot 16}{64^2}$, $00000000 \to 00000000, p_3 = 1$, $000006c0 \to 02000000, p_2 = \frac{12 \cdot 16}{64^2}$, $02000000 \to 40004010, p_1 = \frac{14}{64}$, with total probability $p = \frac{1}{9511}$. In the 0-*R attack*, request $\frac{m}{p}$ pairs with $\Delta P = \Omega_P$. Approximately m pairs survive. Given "right pairs," $(P_1, P_2), (C_1, C_2)$, we obtain 5-bits of key from subkey K_5, using the active S-box, S_2, as follows. Try all 2^5 key candidates as a guess and calculate S'_2, if this is not 7 discard. 14 pairs survive. Another right pair reduces this to 2 after $3-5$ right pairs, we're done. A wrong pair satisfying $\Omega_P \to \Omega_T$ occurs with probability 2^{-64}. We can actually do the first and last rounds simultaneously to get 10 key-bits. To calculate m, notice that we get about $2^{-64}\frac{m}{p}$ "wrong pairs" ("WP") and the total number of suggested wrong keys suggested is $2^{-54}\frac{m}{p}$ which is negligible for $m < 2^{36}$. Since there are 196 subkeys suggested 14^2 values, "right pair" must agree on the 2 shared bits, so $\frac{1}{4}$ of these survive this filter leaving 49 subkeys on average. The right key is always among then. A wrong key is suggested $\frac{48}{1023}m = .05m$ times. If t is the threshold for picking the key, $m = 2, t = 2$ succeeds .276 of the time, $m = 4, t = 3$ succeeds .53 of the time and $m = 5, t = 3$ succeeds .64 of the time and $m = 10, t = 5$ succeeds .91 of the time. In the 1-*R attack*, $f' = (400046D0)$ enters F in sixth round and the pattern ?000???? must emerge this gives a $32 + 12 = 44$ bit filter so given 40000 pairs, we expect $40000 \cdot 2^{-44} < 2^{-28}$ WP's to survive the filter. Now examine the input difference. In the 2-*R attack*,

request 100000 pairs. Output of F in seventh round is $C'_L \oplus (400046D0)$ and only 7 bits after round 7 are known. All right pairs suggest the correct key in round 7. We expect 33 to suggest keys and 4^8 subkeys to be suggested per pair. $33 \cdot 2^{16} \approx 2^{21}$ suggestions and wrong keys are suggested $\frac{2^{21}}{2^{48}} = 2^{-27}$ times. For linear $1R$, guess subkey on last round and use distinguisher to confirm. Ask for $N = cq^{-2}$ encryptions.

Linear cryptanalysis: $\alpha \cdot P \oplus \beta \cdot C = \gamma \cdot C$ with $p = \frac{1}{2} + \delta$ requires about $c\delta^{-2}$ plaintexts. Last round estimation: $L(P) \oplus M(C) \oplus N(P_{n-1}, K_n) = P(K)$ then use MLE: T= # plain cipher pairs = 0 if $|T_{max} - \frac{N}{2}| > |\frac{N}{2} - T_{min}|$ and $p > .5$, guess $P(K) = 0$.

Basic Linear constraints in DES:

-	SBx	SBox Equation	Round Equation	Prob
A	5	$X[2] \oplus Y[1,2,3,4] = K[2] \oplus 1$	$X[17] \oplus Y[3,8,14,25] = K[26] \oplus 1$	$\frac{52}{64}$
B	1	$X[1,4,5,6] \oplus Y[1,2,3] = K[1,4,5,6] \oplus 1$	$X[1,2,4,5] \oplus Y[3,8,14,25] = K[2,3,5,6] \oplus 1$	$\frac{42}{64}$
C	1	$X[2] \oplus Y[1,2,3,4] = K[2] \oplus 1$	$X[3] \oplus Y[17] = K[4] \oplus 1$	$\frac{34}{64}$
D	5	$X[2] \oplus Y[1,2,3] = K[2] \oplus 1$	$X[17] \oplus Y[8,14,25] = K[26]$	$\frac{42}{64}$
E	5	$X[1,5] \oplus Y[1,2,3] = K[1,5] \oplus 1$	$X[16,20] \oplus Y[8,14,25] = K[25,29] \oplus 1$	$\frac{48}{64}$

Using round bit-numbering (and taking into account expansion and permutation), the relation $S_5(x_1 + k_1, x_2 + k_2, x_3 + k_3, x_4 + k_4, x_5 + k_5, x_6 + k_6) + x_2 = k_2$ becomes $X[17] \oplus Y[3,8,14,25] = K[26] \oplus 1$.

Best Differential attack on full DES: Use $0 \rightarrow 0$ together with 6 concatenated 2-round iterative differential characteristic with $p = \frac{1}{234}$ to obtain a 13 round with $p = 2^{-47.2}$. Use 2R attack on last two rounds. For first round, we want 19600000||00000000 entering round 2. If we get 19600000 to enter the F-function, the output has 20 0 bits and 12 unknown bits. Chose plaintexts so that all possible 2^{12}-bit combinations occur in the 12 bits on corresponding input plaintext. Now choose $2^{35.2}$ such 12 bit structures to insure $2^{47.2}$ pairs. Analyze 2^{24} with difference 19600000 in the right hand word yielding 19600000||00000000 after round 14. Candidate round 16 pairs will have 20 ciphertext bits with 0 difference. Consider $2^{24} \cdot 2^{-20}$ of these. An additional filter is used noting that S_1 with an input difference of 3 can only produce 15 outputs and do the same for round 16 leaving a survival ratio of 0.0745 or 1.19 pairs from each of the $2^{35.2}$ structures. Of the survivors, analyze the output obtaining the key values for which it can be a "right" pair. There are 52 involved bits and 2^{52} key values. Ratio of values that are not discarded in round 16 analysis is $\frac{2^{-32}}{(.8)^8}$. Probability that it is not discarded in round 1 or round 15 analysis is $\frac{2^{-12}}{\frac{13}{16} \cdot \frac{14}{16} \cdot \frac{15}{16}}$. So a key has probability of $.84 \times 2^{-52}$ of being suggested, yielding $1.19 \times .84 \approx 1$ key suggestion. Now try 2^4 possible values for the remaining key to confirm. There are actually two such iterative differential characteristics reducing the complexity by a factor of 2.

Best Linear attack on full DES: Use the 14 round approximation with bias $2^{-21.75}$ twice (once in reverse order). The basic attack is: (1) Ask for the encryption of m random texts. (2) for each of the 24 guessed bits entering active S-Boxes in first and last round, partially encrypt and decrypt and store values of pairs satisfying the approximation. (3) Guess suggested key with maximal deviation from $\frac{m}{2}$. This would normally involve a work factor of $2^{43} \times 2^{24}$ trial encryptions $\times$ 4 S-boxes/128 $= 2^{62}$ but this is reduced to $2 \cdot (2^{43} \times 2^{12} \times 2/128 = 2^{47}$ by doing each approximation seperately and doing the trial encryption once for each of the 2^{12} possible S-box inputs. This gives 26 bits $24 + 2$ from the approximation with probability .85 and the other 30 bits are tried at random.

Note: Suppose $\vec{f} : GF(2)^k \times GF(2)^n \rightarrow GF(2)^n$. If $\vec{f}(\vec{k}, \vec{x}_0) = (1, 1, \ldots, 1)$ then $g(\vec{k}, \vec{x}) = \prod_{i=1}^{n} f_i(\vec{k}, \vec{x})$ is

0 everywhere except $\vec{x} = \vec{x}_0$.

Basic Correlation matrix definitions: Let $f, g : GF(2)^n \to GF(2)$, define $C(f,g) = 2Prob[f(x) = g(x)] - 1$, $\hat{f}(x) = (-1)^{f(x)}$, $\langle \hat{f}, \hat{g} \rangle = \sum_x \hat{f}(x)\hat{g}(x)$, $||\hat{f}|| = \sqrt{\langle \hat{f}, \hat{f} \rangle}$. Note that $C(f,g) = \frac{\langle \hat{f}, \hat{g} \rangle}{||\hat{f}|| \cdot ||\hat{g}||}$. For $u \in GF(2)^n$ define $L_u(x) = u^T \cdot x$ then $\langle \hat{L}_u, \hat{L}_v \rangle = 2^n \delta(u \oplus v)$. With this notation, the (normalized) *Walsh transform* is $F(w) = 2^{-n} \sum_x (-1)^{f(x) \oplus L_w(x)} = 2^{-n} \langle \hat{f}, \hat{L}_w \rangle$. Note that $\hat{f}(x) = \sum_w \frac{\langle \hat{f}, \hat{L}_w \rangle}{||\hat{L}_w|| \cdot ||\hat{f}||} \hat{L}_w(x)$ or $\hat{f}(x) = \sum_w F(w) \hat{L}_w(x)$. Denote $\mathcal{W}(f) = F$ and note that $\sum_w F(w)^2 = 1$. If $\mathcal{BF}_n$ denotes the boolean functions from $GF(2)^n$ to $GF(2)$, we can define a map $\mathcal{L} : \mathcal{BF}_n \to \mathbb{R}^{2^n}$ by $f \mapsto ((-1)^{f(0,\ldots,0)}, (-1)^{f(0,\ldots,1)}, \ldots, (-1)^{f(1,\ldots,1)})$. If $f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), f_2(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$ then define the $m \times n$ *correlation matrix* as $C^{(f)} = (c_{u,w}), c_{u,w} = C(u \cdot f(x), L_w)$.

Fast Hadamard Transform: $H_{2^m} = H_2 \otimes H_{2^{m-1}}$. $H_{2^m} = M_{2^m}^{(1)} M_{2^m}^{(2)} \ldots M_{2^m}^{(m)}$, $M_{2^m}^{(i)} = I_{2^{m-1}} \otimes H_2 \otimes I_{2^{i-1}}$.

Observation: A *balanced boolean function* is uncorrelated with either constant function. *Question:* What is the best affine approximation of a balanced function? The question is important because if $E(k,x)$ is a block cipher on blocks of n bits, each $E_i(k,x)$ is a balanced boolean function. How many inputs satisfy all approximations? For the correct input, what are the expected number of equations that agree with it? Variance, etc.

Theorem: $\sum_w F(w) = \pm 1$.

Proof: $\sum_w F(w) = \sum_w 2^{-n} \sum_x (-1)^{f(x)+w \cdot x} = 2^{-n} \sum_x (-1)^{f(x)} (\sum_w (-1)^{w \cdot x}) = 2^{-n} \sum_x (-1)^{f(x)} 2^n \delta_{w,x}$, so $\sum_x (-1)^{w \cdot x + c} = (-1)^c, w = 0, 0, w \neq 0$. Let $F(w,c) = \sum_x (-1)^{f(x+w \cdot x+c)}$ then $\sum_{w,c} F(w,c) = 0$.

Theorem: If $h(x) = f(x) \oplus g(x)$ then $H(w) = \sum_v F(v \oplus w) G(v)$. If $h(x) = f(x) \cdot g(x)$ then $\hat{h}(x) = \frac{1}{2}(1 + \hat{f}(x) + \hat{g}(x) - \hat{f}(x) \cdot \hat{g}(x))$ and hence $H(w) = \frac{1}{2}(\delta(w) + \mathcal{W}(f) + \mathcal{W}(g) - \mathcal{W}(f \oplus g))$.

Proof: Let $N = 2^n$. $\sum_u F(u) G(w+u) = \sum_u (\frac{1}{N} \sum_s (-1)^{f(s)+s \cdot u}) (\frac{1}{N} \sum_t (-1)^{g(t)+t \cdot (w+u)}) = \sum_u (\frac{1}{N^2} \sum_t (-1)^{f(s)} (-1)^{g(t)} (-1)^{t \cdot w} (-1)^{(s+t) \cdot u}) = (\frac{1}{N^2}) \sum_t (-1)^{f(s)} (-1)^{g(t)} (-1)^{t \cdot w} (\sum_u (-1)^{(s+t) \cdot u})$. The last sum is 0 unless $s = t$ in which case it's N so $\sum_u F(u) G(w+u) = \frac{1}{N} \sum_t (-1)^{f(t)+g(t)+w \cdot t}$.

Theorem: If $V = V_1 \oplus V_2$, $f(u_1 + u_2) = f(u_1)$ and $g(u_1 + u_2) = g(u_2)$ for $u_1 \in V_1, u_2 \in V_2$ and $h(x) = f(x) \oplus g(x)$ then $H^{(V)}(u_1 + u_2) = F^{(V_1)}(u_1) G^{(V_2)}(u_2)$. For example, $h(x,y) = (f(x), g(y))$, $C^{(h)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ F(0) & F(1) & 0 & 0 \\ G(0) & 0 & G(1) & 0 \\ F(0)G(0) & F(1)G(0) & F(0)G(1) & F(1)G(1) \end{pmatrix}$.

Theorem: If $C^{(f)}$ is invertible, $(C^{(f)})^{-1} = (C^{(f)})^T$.

Proof: If h is invertible, $(C^{(h)})^{-1} = (C^{(h)})^T$. For a bijection, $C(u^T h^{-1}(a), w^T a) = C(u^T b, w^T h(b)) = C(w^T h(b), u^T b)^T$, so, $C^{(h^{-1})} = (C^{(h)})^{-1}$.

Theorem: f is invertible iff $C^{(f)}$ is invertible.

Proof: The $\to$ direction follows from the inverse formula above. The proof of $\leftarrow$: $(-1)^{u^T h(a)} = \sum_w C_{u,w}^{(h)} (-1)^{w^T a}$. If $C^{(h)}$ is invertible, $(-1)^{w^T a} = \sum_u (C^{(h)})_{w,u}^{-1} (-1)^{u^T h(a)}$. If $\exists x \neq y : h(x) = h(y)$, substituting into the equation above, $(-1)^{w^T x} = (-1)^{w^T y}$ and that is just wrong.

Theorem: If $h(x) = f(g(x))$ then $C^{(h)} = C^{(f)}C^{(g)}$.

Proof: $(-1)^{u^T \cdot h(a)} = \sum_v C^{(f)}_{u,v}(-1)^{v^T \cdot g(a)} = \sum_v C^{(f)}_{u,v}(\sum_w C^{(g)}_{v,w}(-1)^{w^T \cdot a})$.

Theorem: If $h(x) = x \oplus a$ then $C^{(f)}_{u,u} = (-1)^{u^T \cdot a}$.

Proof: $u^T \cdot h(a) = u^T \cdot x \oplus u^T \cdot a$.

Theorem: If $h(x) = Mx$ then $C^{(f)}_{u,w} = \delta(M^T u \oplus w)$.

Proof: $u^T \cdot h(a) = (M^T u)^T a$.

Theorem: $C_{u\oplus v,x} = \sum_w C_{u,w\oplus x}C_{v,w}$.

Proof: $\mathcal{W}((u \oplus v)^T h(a)) = \mathcal{W}(u^T h(a)) \otimes \mathcal{W}(v^T h(a))$; note that first transform on right is $C^{(h)}_{u,w}$ and second is $C^{(h)}_{v,w}$. One consequence is: $C_{u\oplus v,0} = \sum_w C_{u,w}C_{v,w}$.

Theorem: A Boolean transformation is invertible iff every output parity is a balanced binary boolean function of the input bits.

Proof: Let $C = C^{(h)}$. $\rightarrow$: If h is invertible, $CC^T = I$, $C_{00} = 1$ and the norm of every row and column is 1. $C(u^T h(a), 0) = \delta(u)$; all rows except row 0 are correlated to 0 hence the function is balanced for $u \neq 0$. For $\leftarrow$: The condition on output parities being balanced is $C_{u,0} = 0, u \neq 0$. i.e.- C is orthogonal. $CC^T = I \leftrightarrow \sum_w C_{u,w}C_{v,w} = \delta(u \oplus v)$ ("*") also $\sum_w C_{u,w}C_{v,w} = C_{u\oplus v,0}$ but $C_{u,0} = 0, u \neq 0$ and $C_{00} = 1$ so "*" holds $\forall u, v$ hence C is orthogonal and invertible so by the previous result h is invertible.

Theorem: Let u and w are parities then and F^u denotes the normalized Walsh transform of $u^T \vec{f}(\vec{x})$ while G^w denotes the normalized Walsh transform of $w^T \vec{g}(\vec{x})$ then $(C(\vec{f}, \vec{g}))_{u,w} = \sum_v F^u(v)G^w(v)$.

Definition: A *linear trail* is $U = (u_0, u_1, \ldots, u_r)$ associated with a composite function $\beta = \rho_r\rho_{r-1}\ldots\rho_1$ with correlation contribution at each step of $C((u_i^T \rho_i(a), u_{i-1}a)$ and overall correlation of $C_p(U) = \prod_i C^{\rho_i}_{u_i,u_{i-1}}$.

Theorem: $C(u^T\beta(a), w^T a) = \sum_{U,u^{(0)}=u,u^{(r)}=w} C_p(U)$.

Proof: Follows from definition.

Theorem: The correlation coefficients and spectrum values for a boolean function over $GF(2)$ are integer multiples of 2^{1-n}.

Proof: The values are of the form $k + (2^n - k)(-1) = 2k - 2^n$ which is even.

Theorem: The correlation $\hat{c}_{fg}(b) = C(f(x), g(x \oplus b)) = \mathcal{W}^{-1}(FG)$.

Proof: $\hat{c}_{fg}(b) = 2^{-n}\sum_a (-1)^{f(a)\oplus g(a\oplus b)} = C(f(x), g(x \oplus b))$.

"Bricklayer" functions: If

$$h(a(1), \ldots, a(n)) = (h(1)(a(1), a(2), \ldots, a(n)), h(2)(a(1), a(2), \ldots, a(n)), \ldots, h(n)(a(1), a(2), \ldots, a(n))),$$

then $C^{(h)}_{uv} = \prod_{i=1}^n C^{h(i)}_{u_i,v_i}$.

Truncating Function: Let $a' = \varphi^{v,\epsilon,s}(a)$ taking $\varphi : GF(2)^{n-1} \rightarrow GF(2)^n$ be defined by $a'_i = a_i$ for $i \neq s$

and $a'_s = \epsilon \oplus v^t a \oplus a_s$ where $v^T a = \epsilon$ defined the restriction. Then $C^{\varphi}_{w,w} = 1$, $C^{\varphi}_{v\oplus w,w} = (-1)^{\epsilon}$, $\forall w : w_s = 0$; note there are two non-zero entries both of amplitude 1. If $C' = CC^{\varphi}$, $C'_{u,w} = C_{u,w} \oplus (-1)^{\epsilon} C_{u,v\oplus w}$ if $w_s = 1$ and 0 if $w_s = 0$.

Theorem: For *key alternating ciphers*, $C_p(U) = \prod_i (-1)^{u_i^T k_i} C_{u_i,u_{i-1}} = (-1)^{d_U \oplus \bigoplus_i u_i^T k_i} |C_p(U)|$ where $d_U = 1$ if $\prod_i (-1)^{u_i^T k_i} C_{u_i,u_{i-1}} < 0$ and 0 otherwise.

Theorem: $C(v^T \cdot \beta(a), w^T a) = \sum_{U,u_0=u,u_r=w} (-1)^{d_U \oplus U^T K} |C_p(U)|$.

Put $s_i = U^T K \oplus d_U$ and $C_i = C_p(U_i)(-1)^{s_i}$, then averaging over the round keys, for all trail, we get:

Theorem: $E(C_t^2) = 2^{-n_K} \sum_k (\sum_i (-1)^{s_i} C_i)^2$.

Proof: $E(C_t^2) = 2^{-n_K} \sum_k (\sum_i (-1)^{U_i^T k \oplus d_{U_i}} C_i)^2 = 2^{-n_K} \sum_i \sum_j (\sum_k (-1)^{(U_i \oplus U_j)^T k \oplus d_{U_i} \oplus d_{U_j}} C_i C_j)$.
But $C_i C_j = 2^{n_K} \delta(i \oplus j)$.

For key schedule $K = M_\kappa(k)$, $E(C_t^2) = 2^{-n_K} \sum_i \sum_j (\sum_k (-1)^{(d_{U_i} \oplus d_{U_j})^T M_\kappa k \oplus d_{U_i} \oplus d_{U_j}}) C_i C_j$. The inner sum simplifies to $(-1)^{d_{U_i} \oplus d_{U_j}} 2^{n_K} \delta(M_\kappa^T (U_i \oplus U_j))$. If key schedule is not linear $K = f_\kappa(k)$, the coefficient of the mixed term is $(-1)^{(U_i \oplus U_j)^T f_\kappa(k) \oplus d_{U_i} \oplus d_{U_j}}$.

Observation: Multiround linear expressions correspond to linear trails. Generally, $|C_p(U)|$ is independent of round key but this is not the case in DES because of the shared bits between S-boxes. 32 bit input parities before E give rise to α 2^{2l}-48 bit patterns. If l is the number of pairwise neighboring S-boxes, we can do this in $16l$ multiplications and additions. The probability that a multiround expression holds is $\frac{1}{2}(1 + C_p(U))$ for the associated trail.

Observation: All Hadamard transform values of *bent functions* are equal to $\pm 2^{\frac{m}{2}}$ and hence the distance to any affine function is $2^m \pm 2^{\frac{m}{2}-1}$. If $f(x_1, x_2, \ldots, x_m)$ is bent and $m \geq 6$ then f is indecomposable. $f(u_1, \ldots, u_m, v_1, \ldots, v_m) = g(v_1, \ldots, v_m) + \sum_i u_i v_i$ is bent. If $f(u_1, \ldots, u_m, v_1, \ldots, v_m) = \sum_i u_i v_i$, then $f + u_1 u_2, u_3$, $f + u_1 u_2, u_3 u_4$, $\ldots$, $f + u_1 u_2, u_3 \ldots u_m$ are all inequivalent bent functions.

Correlation Immunity: In this paragraph, F denotes the unnormalized Walsh transform of f. A function $z = f(x_1, \ldots, x_n)$ on n variables $x_1, \ldots, x_n$ is m-th order *correlation immune* if for every subset of these variables or size m, $I(z; x_{i_1}, \ldots, x_{i_m}) = 0$. If f has correlation immunity m and non-linear order k, $m+k \leq n$. Let $N_{ab}(\omega) = |\{x : z = f(x) = a, \omega \cdot x = b\}|$ then $F(\omega) = N_{10}(\omega) - N_{11}(\omega)$. Denote $p_a = P(z = a)$ then $P(\omega \cdot x = b | z = a) = \frac{P(\omega \cdot x = b, z = a)}{P(z=a)} = p_a^{-1} 2^{-n} N_{ab}(\omega)$. We obtain the following: $P(\omega \cdot x = 0 | z = 1) = \frac{1}{2} + p_1^{-1} 2^{-n-1} F(\omega)$, $P(\omega \cdot x = 1 | z = 1) = \frac{1}{2} - p_1^{-1} 2^{-n-1} F(\omega)$, $P(\omega \cdot x = 0 | z = 0) = \frac{1}{2} + p_0^{-1} 2^{-n-1} F(\omega)$, $P(\omega \cdot x = 1 | z = 0) = \frac{1}{2} - p_0^{-1} 2^{-n-1} F(\omega)$. Let $h(t) = -tlg(t) - (1-t)lg(1-t)$.
Theorem 1: Let $x_0, \ldots, x_{n-1}$ be independent and uniformly distributed arguments of the boolean function f whose output is the random variable z; then $\forall \omega \neq 0, I(z; \omega \cdot x) = 1 - p_0 h(\frac{1}{2} - \frac{F(\omega)}{2^{n+1} p_0}) - p_1 h(\frac{1}{2} - \frac{F(\omega)}{2^{n+1} p_1})$. Moreover, when z is uniformly distributed then $I(z; \omega \cdot x) = 1 - h(\frac{1}{2} - 2^{-n} F(\omega))$. F thus describes the best affine approximation of f (pick ω with largest coefficient, the coefficients of the best affine approximation has coefficients of 1 for the corresponding variables). This generalizes to
Theorem 2: Let $x_0, \ldots, x_{n-1}$ be independent and uniformly distributed arguments of the boolean function $f_i \in \mathcal{F}$ where $\mathcal{F} = \{f_1, \ldots, f_m\}$, $p_f = \frac{1}{m}$ and the outputs of the randomly selected f_i is the random variable z; then $\forall \omega \neq 0, I(z; \omega \cdot x) = 1 - p_0 h(\frac{1}{2} - \frac{\sum_{i=1}^m F_i(\omega)}{2^{n+1} m p_0}) - p_1 h(\frac{1}{2} - \frac{\sum_{i=1}^m F(\omega)}{2^{n+1} m p_1})$. Moreover, when z is uniformly distributed then $I(z; \omega \cdot x) = 1 - h(\frac{1}{2} - 2^{-n+1} m^{-1} \sum_{i=1}^m F_i(\omega))$. Again, this provides the best affine ap-

proximation for the set of functions. Finally, this implies **Theorem 3:** A boolean function f is correlation immune of order m if $F(\omega) = 0, \forall \omega : 1 \leq wt(\omega) \leq m$.

Counting Results: Let $N = 2^n$ and $BF(n)$ denotes the set of boolean functions on n-bit values then $|BF(n)| = 2^N$. Let $BBF(n)$ be the balanced functions on n bits then $|BBF(n)| = \binom{N}{\frac{N}{2}}$, $|GA(n)| \approx 2^{m^2+m}$.

The natural isomorphism: $\mathcal{L} : GF(2)^n \to \mathbb{R}^{2^n}$ by $a \mapsto (-1)^{a^T \cdot x}$. $\mathcal{L}(a+b) = \mathcal{L}(a)\mathcal{L}(b)$ by pointwise multiplication. Almost directly from the definitions, we get **Theorem:** $C^{(h)}(\mathcal{L}(a)) = \mathcal{L}(h(a))$.

Theorem: The elements of a correlation matrix corresponds to an invertible transform of n-bit vectors are integer multiples of 2^{2-n}. The proof uses the restriction map and the fact that $\sum (F(w)+F(w+v))^2 = 2$.

Theorem: Let $F_q, q = 2^n$, $Tr_{F_q/F_2}(x) = Tr(x) = \sum_{i=0}^{n-1} x^{2^i}$. $Tr(x) \neq 0$ for some x. $Tr(x+y) = Tr(x) + Tr(y)$. $Tr(x^2) = Tr(x)$. $Tr(x) \in F_2$. $Tr(\omega x)$ is linear in x. $Tr(\omega_1 x) = Tr(\omega_2 x) \to \omega_1 = \omega_2$. $Tr(\omega x)$ are exactly the linear functions.

Definition: $F : F_{2^n} \to F_{2^m}$ is *differentially δ uniform* if $\forall \alpha, \beta, \alpha \neq 0$: $|\{x : F(x+\alpha) + F(x) = \beta\}| \leq \delta$. **Theorem:** $F(x) = x^{2^k+1}$, $s = (k,n)$ then F is differentially 2^s-uniform. $N(F) = 2^{n-1} - 2^{\frac{n+s}{2}-1}$. **Theorem:** Let $G(x) = x^{-1}, x \neq 0; 0, x = 0$. F is differentially 4 uniform. $N(G) \geq 2^{n-1} - 2^{\frac{n}{2}}$.

Boolean functions: $a \vee b = a \oplus b \oplus ab$ as a boolean function. Let $\vec{x} = (x_4, x_3, x_2, x_1)$ with x_1 the least significant bit. $\vec{F}(\vec{x}) = (F_4(\vec{x}), F_3(\vec{x}), F_2(\vec{x}), F_1(\vec{x}))$. If $\rho = (0000, 0001)$ then $\vec{F_i^{\rho}}(\vec{x}) = x_i, i > 1$ and $\vec{F_1^{\rho}}(\vec{x}) = (\overline{x_2 \vee x_3 \vee x_4})(x_1 \oplus 1) \oplus (x_2 \vee x_3 \vee x_4)x_1 = 1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_2x_3x_4$. If $\sigma = (0000, 0001, \ldots, 1111)$, then $\vec{F_1^{\sigma}}(\vec{x}) = x_1 \oplus 1$, $\vec{F_2^{\sigma}}(\vec{x}) = x_1(x_2 \oplus 1) \oplus \overline{x_1}x_2 = x_1 \oplus x_2$, $\vec{F_3^{\sigma}}(\vec{x}) = (x_1x_2)(x_3 \oplus 1) \oplus (\overline{x_1x_2})x_3 = x_1x_2 \oplus x_3$, $\vec{F_4^{\sigma}}(\vec{x}) = (x_1x_2x_3)(x_4 \oplus 1) \oplus (\overline{x_1x_2x_3})x_4 = x_1x_2x_3 \oplus x_4$.

Theorem: $RM(r,m)$ has minimum distance 2^{m-r}. $R(1,5)$ has 48 inequivalent affine classes.

Balence: Each possible Boolean transformation on n bits is a permutaion on the $2^n, n$-bit values and so listing them in order, the columns are the possible $\vec{f}$ vectors representing the component functions. If we label these as points in $GF(2)^{2^n}$ and draw an edge between allowable co-components with the edges labeled by the correlation between these vectors, any allowable n boolean functions form a complete graph with the label 0 on each edge. $C(f,g) = 1 - \frac{wt(f+g)}{2^{n-1}}$. **Generalized Balence Theorem:** For each $n \leq 128$ and each $1 \leq b_1 < b_2 < \ldots < b_n \leq 128$ and fixed $\vec{k}$, $(E_{b_1}(\vec{k}, \vec{x}), E_{b_2}(\vec{k}, \vec{x}), \ldots, E_{b_n}(\vec{k}, \vec{x}))$ takes each value in $\mathbb{Z}_2^n$ as $\vec{x}$ varies over $\mathbb{Z}_2^n$. So does any non-trivial sum of any of these functions. **Theorem:** If $f : GF(2)^{n-1} \to GF(2)$ is any boolean function, $g(x_1, \ldots, x_n) = f(x_1, \ldots, x_{n-1}) + x_n$ is balanced.

Advantage: Write $\epsilon = E_K$ and $\epsilon' = E_{K'}$. What does $[\epsilon^i, \epsilon'^j]$ reveal about K for known K'. Let $\mathcal{P} = \{p_1, p_2, \ldots, p_m\}$ and let l be given put $N = p_1^l \ldots p_m^l$ and denote the set of n-bit elements of the block by S; what is $\mathbb{C}_S(\epsilon^N)$? How do you characterize the $x : g(x) = x$ where, say, g represents N applications of ϵ. In general, ϵ is complicated but $\epsilon^m = 1$ for some m and ϵ^t many be much simpler for some $m < t$. Let $g_{(i)}^{(0)}(x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = f(x_1, x_2, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$. **Idea:** Suppose ϵ^i and ϵ^j are relatively easy to determine (low degree, good approximation whatever) and $(i,j) = 1$ then we can find $a, b : ai + bj = 1$ and calculate $\epsilon = (\epsilon^i)^a (\epsilon^j)^b = \epsilon$. Let $B_n(r, \vec{v}) = \{\vec{x} : wt(\vec{v} \oplus \vec{x}) = r\}$. $|B_n(\vec{v}, r)| = 2^{n-r}$. Motivation for idea is while there are lots of "far away" approximations of ϵ there aren't many near ones. However, there may be close approximations of ϵ^i.

Theorem: Let f be the Boolean function defined by $S_f^0 = \{x : f(x) = 0\}$ and $S_f^1 = \{x : f(x) = 1\}$. If $e_i(x) = E_i(k, x)$ then $|S_{e_1}^b \cap S_{e_2}^b \cap \ldots \cap S_{e_k}^b| = 2^{n-k}$. What are the permutations that fix such a set?

Theorem: Let $f, g : GF(2)^n \to GF(2)$ and $N = 2^n$. Let a be the number of positions where f and g agree and d be the number of positions where f and g disagree, then $Pr[(f(x) = g(x)] = \frac{a}{2^n}$. Note that $wt(f \oplus g) = d = dist(f, g)$. Now suppose $g(x) = w \cdot x$, the linear function. $F(w) = \frac{1}{2^n}\sum_x (-1)^{f(x)=g(x)} = \frac{1}{2^n}(a-d)$ Since $a + d = 2^n$, $F(w) = 2\frac{a}{2^n} - 1$ and thus $C(f, w) = F(w)$. These yield $dist(f(x), w \cdot x) = 2^n(1 - F(w))$. Thus the best affine approximation is the one which maximizes $|F(w)|$ for some w.

Theorem: Now let $f : GF(2)^n \to GF(2)$ be a bijective boolean transformation with component functions $f_1, f_2, \ldots, f_n$. All such transformations represent permutations in S_{2^N} and the correlation matrices of these transformations is orthogonal ($CC^T = I$). A block cipher gives rise to such transformations by setting $f(x) = E_K(x)$ for fixed K. Note that all balanced boolean functions can be obtained by applying a permutation in S_{2^N} to a sequence of $\frac{N}{2}$, 1's and $\frac{N}{2}$, 0's.

Theorem 1: With the foregoing notation, $C(f_i, 1) = C(f_i, 0) = 0$, $C(f_i, f_j) = 0, i \neq j$, $wt(f_i) = 2^{n-1}, \forall i$, $wt(f_i f_j) = 2^{n-2}, i \neq j$ and in general, $wt(f_{i_1} f_{i_2} \ldots f_{i_k}) = 2^{n-k}$. Further, $C(f_i f_j, f_k) = \frac{1}{2}$, $C(f_i, f_j, f_k f_l) = C(f_i f_j f_k, f_l)$ and in general $C(f_{i_1} f_{i_2} \ldots f_{i_k}, f_l) = 2^{n-k-1}$. Let f be a boolean function. **Theorem 2:** Let f be a boolean function. The N functions $f_{i_1} f_{i_2} \ldots f_{i_k}$ form a basis for the space of boolean functions; that is, for any boolean function g, $\exists a_{i_1,i_2,\ldots,i_k}^{(g)}$ such that $g(x) = \sum_{1 \leq i_1 < i_2 < \ldots < i_k = n} a_{i_1,i_2,\ldots,i_k}^{(g)} f_{i_1} f_{i_2} \ldots f_{i_k}$. In particular, there are such coefficients such that $x_i = \sum_{1 \leq i_1 < i_2 < \ldots < i_k = n} a_{i_1,i_2,\ldots,i_k}^{(x_i)} f_{i_1} f_{i_2} \ldots f_{i_k}$. Define $Appx_i(f) = \{g : dist(f, g) \leq i\}$, then $|Appx_i(f)| = \sum_{j=0}^{i} \binom{N}{i}$.

$NL(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$, $NL(f) \leq 2^{n-1} + \sqrt{2^n + max_{e \neq 0}(F(D_e(f)))}$, where $D_e f = f(x) \oplus f(x \oplus e)$.

Theorem (Rothaus): Let $n \geq 4$ of even algebraic degree then any bent function on $GF(2)^n$ has degree $\leq \frac{n}{2}$. An n-Boolean function, f, is m-resilient iff f is balanced and $F(u) = 0, \forall u : wt(u) \leq m$. Maiorana-MacFarland class $\mathcal{M} = \{f : f(x, y) = x\pi(y) \oplus g(y)\}$ where π is a permutation on $GF(2)^{\frac{n}{2}}$ and g is affine. $|\mathcal{M}| = (2^{\frac{n}{2}})! 2^{\frac{n}{2}}$. For *bent quadratics*, $\bigoplus_{1 \leq i,j \leq n} a_{ij} x_i x_j \oplus h(x)$, h, affine.

Definition: For this section, $f : GF(2)^m \to GF(2)$. The *sensitivity* of v is defined by $S(v) = |\{v' : f(v) \neq f(v'), dist(v, v') = 1\}|$. The average sensitivity $aS(f) = \frac{1}{2^m}\sum_v S(v)$. The *influence* of x_i is defined by $I(x_i) = Prob(f(x_1, \ldots, x_{i-1}, y, x_{i+1}, \ldots, x_m)$, the probability that the function is determined no matter what y is.

Theorem: Let f be a boolean function of n variables with average sensitivity $aS(f) = k$. Let $\epsilon > 0$ and $M = \frac{k}{\epsilon}$ then (1) $\exists h$ depending on $exp((2 + \sqrt{\frac{2log(4M)}{M}})M)$ variables such that $Prob(f \neq h) \leq \epsilon$; and, (2) $\exists g$ of degree at most $exp((2 + \sqrt{\frac{2log(4M)}{M}})M)$ such that $Prob(f \neq g) \leq \frac{\epsilon}{2}$.

Basic Question: Let F be a family of m binary n-vectors. How densely packed is F? Given $b \leq n$, $|F|$, what is the largest possible number of pairs of vectors in F whose Hamming distance is less than b?

Trace and correlation in $GF(2^n)$: $C_{u,w}^f = 2^{-n}\sum_a (-1)^{Tr(wa)}(-1)^{Tr(uf(a))}$ so the terms are determined by the condition $Tr(wa + uf(a)) = 0$, if this is satisfied by r values the entry is $r2^{1-n}$. If a function is linear over $GF(2^n)$, it is linear over $GF(2)$ but not vice versa.

Theorem: Let r_n be the ratio of the number of invertible $n \times n$ matrices over $GF(2)$ to the number of $n \times n$ matrices over $GF(2)$, then $lim_{n\to\infty}(r_n) \approx 0.288$.

Proof: The number of invertible $n \times n$ boolean matrices is $t_n = (2^n-1)(2^n-2)\dots(2^n-2^{n-1})$. The number of $n \times n$ boolean matrices is 2^{n^2}. $t_n = 2^{\frac{n(n-1)}{2}}(2^n-1)(2^{n-1}-1)\dots(2-1)$. Define $s_n = (2^n-1)(2^{n-1}-1)\dots(2-1)$. Now $t_{n+1} = 2^{\frac{n(n+1)}{2}}s_{n+1} = 2^{\frac{n(n+1)}{2}}2^{-\frac{n(n-1)}{2}}(2^{\frac{n(n-1)}{2}}s_n)(2^{n+1}-1) = 2^n(2^{n+1}-1)t_n$. Dividing both sides of this by $2^{(n+1)^2}$, we get $r_{n+1} = \frac{t_{n+1}}{2^{(n+1)^2}} = \frac{2^n}{2^{2n+1}}\frac{t_n}{2^{n^2}}(2^{n+1}-1) = r_n(1-2^{-(n+1)}))$. Using this recurrence, we get $r_n = \prod_{i=1}^{n}(1-2^{-n})$. The product approaches ≈ 0.288 as $n \to \infty$.

Question: Is there an easy to compute function, T_K, obviously non-linear, so that $T_K E_K T_K^{-1}$ has good linear approximations? How do you find such T_K? Finding the best approximation reduces to finding an orthogonal transformation that maximizes the largest entry. Suppose T is such a matrix; if T has all bad affine approximations is it possible that there is another orthogonal transformation, R with $T^R = R^{-1}TR$ such that $max_{ij}(|(T^R)_{ij}|) > max_{ij}(|(T)_{ij}|)$? If $\rho_1, \rho_2, \dots, \rho_n$ is a series of such transformations (like the iterated components of a block cipher), note that $R^{-1}E_K(x)R = R^{-1}\rho_1 R R^{-1}\rho_2 R \dots R^{-1}\rho_n R$ thus raising the possibility of better "per round" approximations on a related cipher.

Here is a motivating example in $\mathbb{R}^3$: $R = \begin{pmatrix} cos(\varphi) & sin(\varphi) & 0 \\ -sin(\varphi) & cos(\varphi) & 0 \\ 0 & 0 & 1 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & cos(\theta) & sin(\theta) \\ 0 & -sin(\theta) & cos(\theta) \end{pmatrix}$ and

$$R^{-1}TR = \begin{pmatrix} cos^2(\varphi) + cos(\theta)sin^2(\varphi) & cos(\varphi)sin(\varphi) - cos(\theta)cos(\varphi)sin(\varphi) & -sin(\varphi)sin(\theta) \\ -cos(\varphi)sin(\varphi) + cos(\theta)cos(\varphi)sin(\varphi) & sin^2(\varphi) + cos(\theta)cos^2(\varphi) & sin(\varphi)sin(\theta) \\ sin(\varphi)sin(\theta) & -cos(\varphi)sin(\theta) & cos(\theta) \end{pmatrix}$$

$NL(f) \le 2^{n-1} - 2^{\frac{n}{2}-1}$, $NL(f) \le 2^{n-1} + \sqrt{2^n + max_{e\neq 0}(F(D_e(f)))}$, where $D_e f = f(x) \oplus f(x \oplus e)$.

Prolog to computing DES correlation matrix: Let $f(x_1, x_2, x_3, x_4) = (x_1 + f_1(x_3, x_4), x_2 + f_2(x_3, x_4), x_3, x_4)$ (first position most significant) then, with least significant positions indexing rows and columns, and $F_i(w)$ as the Walsh transform for $f_i(x_3, x_4)$ and $H(w)$ the Walsh transform of $h(x) = f_1(x) + f_2(x)$. Bit positions

in this example are (x_1, x_2, x_3, x_4).

$$C^{(f)} = \left(\begin{array}{cccc|cccc|cccc|cccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & F_2(0) & F_2(1) & F_2(2) & F_2(3) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & F_2(1) & F_2(0) & F_2(3) & F_2(2) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & F_2(2) & F_2(3) & F_2(0) & F_2(1) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & F_2(3) & F_2(2) & F_2(1) & F_2(0) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & F_1(0) & F_1(1) & F_1(2) & F_1(3) & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & F_1(1) & F_1(0) & F_1(3) & F_1(2) & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & F_1(2) & F_1(3) & F_1(0) & F_1(1) & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & F_1(3) & F_1(2) & F_1(1) & F_1(0) & 0 & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & H(0) & H(1) & H(2) & H(3) \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & H(1) & H(0) & H(3) & H(2) \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & H(2) & H(3) & H(0) & H(1) \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & H(3) & H(2) & H(1) & H(0)
\end{array}\right)$$

Feistel: A typical round of DES consists of two involutions: τ and σ_k. $\sigma_k(L, R) = (L \oplus f(R, k), R)$, $f(x, k) = PS_1S_2 \ldots S_8(E(x) + k))$. $\tau(L, R) = (R, L)$. First "line" of σ_k is $y_9 = x_9 \oplus S_1^1(x_{64} + k_1, x_{33} + k_2, x_{34} + k_2, x_{35} + k_2, x_{36} + k_2, x_{37} + k_2)$, $y_{17} = x_{17} \oplus S_1^2(x_{64} + k_1, x_{33} + k_2, x_{34} + k_2, x_{35} + k_2, x_{36} + k_2, x_{37} + k_2)$, $y_{23} = x_{23} \oplus S_1^3(x_{64} + k_1, x_{33} + k_2, x_{34} + k_2, x_{35} + k_2, x_{36} + k_2, x_{37} + k_2)$, $y_{31} = x_{31} \oplus S_1^4(x_{64} + k_1, x_{33} + k_2, x_{34} + k_2, x_{35} + k_2, x_{36} + k_2, x_{37} + k_2)$.

Suppose $\tau(x_1, x_2, x_3, x_4) = (x_3, x_4, x_1, x_2)$, with position (0001) representing x_4, then

$$C^{(\tau)} = \left(\begin{array}{cccccccc|cccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right).$$

The column order from left to right in the forgoing is: 1, (x_4), (x_3), (x_4, x_3), (x_2), (x_4, x_2), (x_3, x_2), (x_4, x_3, x_2), (x_1), (x_4, x_1), (x_3, x_1), (x_4, x_3, x_1), (x_2, x_1), (x_4, x_2, x_1), (x_3, x_2, x_1), (x_4, x_3, x_2, x_1) corresponding to the ordered sequence $0000, 0001, 0010, \ldots$. The row order from top to bottom is 1, (x_2), (x_1), (x_2, x_1), (x_4), (x_4, x_2), (x_4, x_1), (x_4, x_2, x_1), (x_3), (x_3, x_1), (x_3, x_2), (x_3, x_2, x_1), (x_3, x_4), (x_3, x_4, x_2), (x_3, x_4, x_2), (x_3, x_4, x_1), (x_3, x_4, x_2, x_1).

Correlation of decomposed function $(g(x_1, x_2, \ldots, x_k, h(x_{k+1}, \ldots, x_n)))$. Minimum distance.

Standard Functions: For $h(x) = x \oplus k$, $C^{(h)}_{u,u} = (-1)^{u^T \cdot k}$. For $h(x) = Mx \oplus w$, $C^{(h)}_{u,w} = \delta(M^T u \oplus w)$. $\hat{c}_{fg} = 2^{-n} \sum_a (-1)^{\hat{f}(a)\hat{g}(a+b)}$, $\hat{r}_f = \hat{c}_{ff}$.

Theorem: All correlation matrices are doubly stochastic and orthogonal. Correlation matrices for involutions are symmetric.

Round correlation for DES: To calculate the *round correlation for DES*, decompose it into three involutions. The first, adds output from odd numbered S-boxes but is otherwise the identity. The second, adds output from even numbered S-boxes but is otherwise the identity. The third transposes L and R. The first and second involutions don't overlap on input variables to the SBoxes so the Walsh transforms of components of the S-Boxes are all that is needed. In both the first and second transformations, each position affected by an S-box is multiplied by $(-1)^{w^T \cdot k}$ (i.e. - ± 1) for the relevant round keys. Thus, if $\sigma_k(L, R) = (L \oplus f(R, k), R)$, $f(x, k) = PS_1S_2 \ldots S_8(E(x) + k))$, the first "line" is $y_9 = x_9 \oplus S^1_1(x_{64} + k_1, x_{33} + k_2, x_{34} + k_2, x_{35} + k_2, x_{36} + k_2, x_{37} + k_2)$, $y_{17} = x_{17} \oplus S^2_1(x_{64} + k_1, x_{33} + k_2, x_{34} + k_2, x_{35} + k_2, x_{36} + k_2, x_{37} + k_2)$, $y_{23} = x_{23} \oplus S^3_1(x_{64} + k_1, x_{33} + k_2, x_{34} + k_2, x_{35} + k_2, x_{36} + k_2, x_{37} + k_2)$, $y_{31} = x_{31} \oplus S^4_1(x_{64} + k_1, x_{33} + k_2, x_{34} + k_2, x_{35} + k_2, x_{36} + k_2, x_{37} + k_2)$. $Tr(C^{(AES)})$ is the number of fixed points of AES. Since $Tr(AB) = Tr(BA)$, $Tr(C^{(AES)}) = Tr(C^{(k_{14})}C^{(k_{13})} \ldots C^{(k_1)}C^{(RS)}(C^{(MRS)})^{13})$.

Differentials: $b = h(a)$, $b^* = h(a^*)$, $b' = b \oplus b^*$ $a' = a \oplus a^*$. $Prob(a', b') = 2^{-n} \sum_a \delta(b' \oplus h(a \oplus a') + h(a))$. This is also called the *difference propagation probability* denoted by $R_p(a' \rightarrow_h b')$ is $Prob^h(a', b') = 2^{-n} \sum_a \delta(b' + h(a + a') + h(a))$; we have $0 \leq R_p(a' \rightarrow_h b') \leq 1$. The *restriction weight* is defined as $w_r(a' \rightarrow_h b') = -lg(R_p(a' \rightarrow_h b'))$ (restriction weight reflect loss of entropy). $w_c(U) = -lg(|C_p(U)|)$ (correlation weight). For bricklayer function, $Prob^h(a', b') = \prod_i Prob^{h_{(i)}}(a'_{(i)}, b'_{(i)})$ and $w_r(a', b') = \sum_i w_r(a'_{(i)}, b'_{(i)})$.

Definition: For the composite function $\beta = \rho_r \circ \ldots \circ \rho_1$, a *differential trail* of length r, is a sequence $Q = (q^{(0)}, q^{(1)}, \ldots, q^{(r)})$ with steps $(q^{(i-1)}, q^{(i)})$ having difference propagation probability $Prob^{\rho_i}(q^{(i-1)}, q^{(i)})$. Each "step" has weight $w_r^{\rho^{(i)}}(q^{(i-1)}, q^{(i)})$. The trail weight is $w_r(Q) = \sum_i w_r^{\rho^{(i)}}(q^{(i-1)}, q^{(i)})$. $Prob(a', b') = \sum_{q^{(0)}=a', q^{(r)}=b'} Prob(Q)$.

Theorem: $\sum_{b'} R_p(a' \rightarrow_h b') = 1$. $Prob(a', b') = 2^{-n} \sum_{u,w} (-1)^{w^T a' \oplus u^T b'} C^2_{u,w}$ and $C^2_{u,w} = 2^{-n} \sum_{u,w} (-1)^{w^T a' \oplus u^T b'} Prob(a', b')$.

Proof: $Prob(a', b') = 2^{-n} \sum_a \delta(h(a) \oplus h(a \oplus a') \oplus b')$
$= 2^{-n} \sum_a \prod_i \frac{1}{2}(-1)^{h_i(a) \oplus h_i(a \oplus a') \oplus b')} + 1$
$= 2^{-n} \sum_a 2^{-m} \sum_u \prod_i \frac{1}{2}(-1)^{u^T \cdot h(a) \oplus h(a \oplus a') \oplus b')}$
$= 2^{-m} \sum_u (-1)^{u^T b'} 2^{-n} \sum_a (-1)^{u^T \cdot h(a) \oplus u^T \cdot h(a \oplus a'))}$
$= 2^{-m} \sum_u (-1)^{u^T b'} \hat{r}_u(a')$
$= 2^{-m} \sum_u (-1)^{u^T b'} 2^{-m} \sum_u 2^{-n} \sum_w (-1)^{w^T a'} C^2_{u,w}$
$= 2^{-m} \sum_u (-1)^{u^T b'} 2^{-m} \sum_{u,w} (-1)^{w^T a' \oplus u^T b'} C^2_{u,w}$

For a differential trail, Q, with weight $< (n-1)$, $Prob(Q) \approx 2^{-w_r(Q)}$ (ignore restriction correlations). For differential trails with $w_r(Q) \geq n - 1$, the right pair will exist only for $2^{n-1-w_r(Q)}$ of the keys.

Block cipher design: To eliminate low weight trails, there are two strategies: (1) Choose S-boxes with difference propagations that have high restriction weight and input-output correlations with high correlation weights; or, (2) Design round transformations so that only trails with many S-boxes occur. Linear cryptanalysis requires correlation $> 2^{-\frac{n_b}{2}}$ over most rounds. This can't happen if we choose the number of rounds so that there are no such linear trails with correlation contribution $> {n_k}^{-1}2^{-\frac{n_b}{2}}$ Each output parity is correlated to an input parity since $\sum_w F(w)^2 = 1$ but if it occurs by constructive interference over many trails that share input/output selection then any such must be the result of at least n_k linear trails which are unlikely to be key dependent. Differential cryptanalysis requires input to output difference propagation with probability $> 2^{1-n_b}$. If there are no differential trails with low weight, difference propagation results from multiple trails which again will not likely be key dependent.

Design strategy for Rijndael: Choose number of rounds so that there is no correlation over all but a few rounds with amplitude significantly larger than $2^{-\frac{n_b}{2}}$ by insuring there are no linear trails with correlation contribution above ${n_k}^{-1}2^{-\frac{n_b}{2}}$ and no differential trails with weight below n_b.

Observation: Examine round transformations $\rho = \lambda \circ \gamma$, where λ is the mixing function and γ is a bricklayer function that acts on bundles of n_t bits. Block size is $n_b = mn_t$. The correlation over γ is the product of correlations over different S-box positions for given input and output patterns. Define weight of correlation as $-lg(Amplitude)$. If output selection pattern is $\neq 0$, the S-box is active. Looking for maximum amplitude of correlations and maximum difference propagation probability. The weight of a trail is the sum of the weights of the selection patterns or the sum of the active S-box positions it is greater than the number of active S-boxes times the minimum correlation weight per S-box. *Wide trail strategy:* design round transformations so there are no trails with low bundle weight.

Definition: Define $w_b(a)$ as the *bundle weight* of a. $\mathcal{B}_d(\phi) = min_{a,b\neq a}(w_b(a \oplus b) + w_b(\phi(a) \oplus \phi(b)))$. $\mathcal{B}_l(\phi, \alpha) = min_{\alpha,\beta,C(\alpha^T x,\beta^T \phi(x))\neq 0}(w_b(\alpha) + w_b(\beta))$.

Theorem: In an alternating key block cipher with $\gamma\lambda$ round functions, the number of active bundles in a two round trail is $\geq$ the bundle branch number of λ. If $\psi = \gamma\Theta\gamma\lambda$ is a four round function, $\mathcal{B}(\psi) \geq \mathcal{B}(\lambda) \times \mathcal{B}^c(\Theta)$ where $\mathcal{B}$ can be either the linear or differential branch number. The linear and differential branch numbers for an AES round is 5.

Linearized polynomial: $L(x) = \sum_{i=0}^{t} \beta_i x^{2^i}, \beta \in GF(2^n)$.

Discrete Fourier Transform: $A_k = \sum[f(x) + f(0)]x^{-k}$, $f(x) = \sum A_k x^k$. $A_{2^i k} = A_k^{2^i}$. Coset leaders: $C_s = \{s, 2s, 2^2 s, \ldots, 2^{n_s-1}s\}$, coset leader s is smallest: $s = s2^{n_s-1} \pmod{2^n - 1}$. For any non-zero function $f : GF(2^n) \to GF(2)$ can be represented as $f(x) = \sum_{k\in\Gamma(n)} Tr_1^{n_k}(A_k x^k) + A_{2^n-1}x^{2^n-1}$ where $\Gamma(n)$ are the coset leaders $\pmod{2^n - 1}$, $n_k \mid n$ and $Tr_1^{n_k}(x)$ is the trace function from $GF(2^{n_k}) \to GF(2)$. Let α be a primitive element of $GF(2^n)$ and $f(0) = 0$ with $a_t = f(\alpha^t), t = 0, 1, 2, \ldots, 2^n - 1$, $x = x_0 + x_1\alpha + x_2\alpha^2 + \ldots + x_{n-1}\alpha^{n-1}$.

Any function $f : GF(2^{n_k}) \to GF(2)$ corresponds to a binary sequence with period $N \mid 2^n - 1$; TBD—what is k. **Hadamard-Walsh:** $\hat{f}(\lambda) = \sum_{x\in GF(2^n)}(-1)^{Tr(\lambda\cdot x)+f(x)}$. Polynomials $\to_{eval}$ Periodic sequences $\leftrightarrow_{trace}$ Boolean Functions.

Definition: By *low degree approximations* we mean $\exists g \neq 0 : fg = 0$ and fg has low degree $deg(fg) \geq deg(f)$. $|S_d| = \sum_{i=0}^{d} \binom{n}{i}$.

Definition: Let f be a boolean function of n variables. The *annihilator ideal* of f, $AN(f) = \{g : g(x)f(x) = 0\}, \forall x \in GF(2^n)$, $AN_d(f) = \{g \in AN(f) : deg(g(x)) \leq d\}$. The *algebraic immunity*, $AI(f)$, is the smallest degree non-zero polynomial in $AN(f) \cup AN(1+f)$. $AI(f) \leq \lceil \frac{n}{2} \rceil$.

NLFSRs: Suppose $\mathcal{L}$ is an n-bit NLFSR based filter generator with filter function f and that L takes the current n-bit state to the next n-bit state. Suppose the initial state is $\vec{x_0}$. Then the generated keystream is $s_t = f \circ L^t(\vec{x_0})$. $s_t = 1$ if $\exists g \in AN_d(f) : g \circ L^t(\vec{x_0}) = 0$, $s_t = 0$ if $\exists h \in AN_d(1+f) : h \circ L^t(\vec{x_0}) = 0$. Collect all functions of degree $\leq d$ for N known keystream bits; then, (1) $g \circ L^t(x_1, x_2, \ldots, x_n) : \forall g \in AN_d(f), \forall 0 \leq t < N : s_t = 1$; and, (2) $h \circ L^t(x_1, x_2, \ldots, x_n) : \forall g \in AN_d(1+f), \forall 0 \leq t < N : s_t = 0$. Using linearization to solve these equations, requires identifying the subset of monomials forming a linear system of up to $\sum_{i=1}^{d} \binom{n}{i}$ variables. Gaussian reduction on this system takes time $O((\sum_{i=1}^{d} \binom{n}{i})^{\omega}) \approx n^{\omega d}$ where $\omega \approx 2.37$ and the the number of monomials is $\approx \frac{2n^d}{d!(dim(AN_d(f))+dim(AN_d(1+f)))}$.

Akelarre: Rounds $0 \leq R < R$. $(B_0, B_1, B_2, B_3) = (A_0, A_1, A_2, A_3) <<< K_{13r+4}[25, 26, \ldots, 31]$. Initial Prep: $I_j = X_j = K_j$. Round r: $(I'_0, I'_1, I'_2, I'_3) = (I_0, I_1, I_2, I_3) <<< K_{13r+4}[25, 26, \ldots, 31]$. $A_R(I'_0 \oplus I'_2, I'_1 \oplus I'_3) = a_L || a_R$. $O_0 = I'_0 \oplus a_R$, $O_1 = I'_1 \oplus a_L$, $O_2 = I'_2 \oplus a_R$, $O_3 = I'_3 \oplus a_L$. Final Out: $Y_j = I'_j + K_{13R+5+j}$. Describe A_R.

FEAL-4: 32 bit blocks, 64 bit keys. Four round Feistel with input/output whitening. Key, K, is used to generate 12 16-bit keys $K_0, K_1, \ldots, K_{11}$. To define the key schedule and the round function F put $G_0(a,b) = (a + b \,(\text{mod } 256)) <<< 2$, $G_1(a,b) = (a + b + 1 \,(\text{mod } 256)) <<< 2$. Key Schedule: Define $f_K : \mathbb{Z}_2^{32} \times \mathbb{Z}_2^{32} \to \mathbb{Z}_2^{32}$ as follows: $f_K(a,b) = c$, $a = a_0||a_1||a_2||a_3$, $b = b_0||b_1||b_2||b_3$, $c = c_0||c_1||c_2||c_3$, then $d_1 = a_0 \oplus a_1$, $d_2 = a_2 \oplus a_3$, $c_1 = G_1(d_1, a_2 \oplus b_0)$, $c_2 = G_0(d_2, c_1 \oplus b_1)$, $c_0 = G_0(a_0, c_1 \oplus b_2)$, $c_3 = G_1(a_3, c_2 \oplus b_3)$. Then put $B_{-2} = 0$, $B_{-1} = K_L$, $B_0 = K_R$, and $B_i = f_K(B_{i-2}, B_{i-1} \oplus B_{i-3})$, $K_{2(i-1)} = (B_i)_L$, $K_{2i-1} = (B_i)_R$. Encryption: If P_L, P_R is the cipher input and C_L, C_R is the cipher output, $L_0 = P_L \oplus (K_4||K_5)$ and $R_0 = L_0 \oplus P_R \oplus (K_6||K_7)$. Each round is defined as: $R_{i+1} = L_i \oplus F((K_{2(i-1)}||K_{2i-1}) \oplus R_i)$ and $L_{i+1} = R_i$. F is defined by: $F(x_0, x_1, x_2, x_3) = (y_0, y_1, y_2, y_3)$ where $y_1 = G_1(x_0 \oplus x_1, x_2 \oplus x_3)$, $y_0 = G_0(x_0, y_1)$, $y_2 = G_0(y_1, x_2 \oplus x_3)$, and $y_3 = G_1(y_2, x_3)$. Finally, $C_L = L_4 \oplus (K_8||K_9), C_R = R_4 \oplus L_4 \oplus (K_{10}||K_{11})$. Note that $A_0 \oplus A_1 = 0x80800000 \to F(A_0) \oplus F(A_1) = 0x02000000$. For differential attack, pick P_L at random and $P_1 = 0x80800000080800000$. Suppose X' is the output differential of F in round 3, Y' is the input differential to F in round 4 and Z' is the output differential in Round 4, then $C'_L = 0x02000000 \oplus Z'$ and $C'_R = C'_L \oplus Y'$ and $Y = C_L \oplus C_R$. Guess K_3 compute Y, Y^* and Z, Z^* and see if differential hold for each guess. analysis, denote $S_{i,j}(X) = x_i \oplus x_j$, $S_i(X) = x_i$. Then, $S_5(G_0(a,b)) = S_7(a \oplus b)$ and $S_5(G_1(a,b)) = S_7(a \oplus b) \oplus 1$. The following hold: $S_{13}(Y) = S_{7,15,23,31}(X) \oplus 1$, $S_5(Y) = S_{15}(Y) \oplus S_7(X)$, $S_{15}(Y) = S_{21}(Y) \oplus S_{23,31}(X)$, $S_{23}(Y) = S_{29}(Y) \oplus S_{31}(X) \oplus 1$ and $a = S_{23,29}(P_L \oplus P_R \oplus C_L) \oplus S_{31}(P_L \oplus C_L \oplus C_R) \oplus S_{31}F(P_L \oplus C_L \oplus K_0)$.

RC4 Weakness: Let S_i be the state at time i, $N = 2^n$ ($n = 8$, usually). Let $\langle z_i \rangle$ be the output sequence. $P(z_2 = 0) = \frac{2}{N}$. [*Proof:* Suppose $S_0[2] = 0$, $S_0[1] \neq 2$, $S_0[1] = X$, $S_0[X] = Y$.] Round 1: $i = 1$, $X = S_0[1] + 0$. Exchange $S_0[1]$ and $S_0[Y]$. Round 2: $i = 2$, $j = X + S_1[2] = X$, Output $S_1[S_1[2] + S_1[X]] = S_1[X] = 0$. So $P(z_2 = 0) \approx \frac{1}{N} + \frac{1}{N}(1 - \frac{1}{N}) \approx \frac{2}{N}$. So by Bayes, if $z_2 = 0$, we can extract byte of state with probability $\frac{1}{2}$.

WEP Attack: WEP is data level encryption using a long term secret K and per message initial vector, IV which is 3 bytes which we call K_0, K_1, K_3. The IV and the key bytes $K_3, \ldots$ form a single RC4 key $K_0, K_1, K_2, K_3, \ldots$. Attack involves selecting $IV = 3|255|V$. The RC4 initialization at $i = 0$ step is $j = j + S_0 + 255 = 3 \,(\text{mod } 256)$ then swap $S[0], S[3]$; this leaves S:

i	0	1	2	3	4	5	6	7	...
S[i]	3	1	2	0	4	5	6	7	...

The $i = 1$ step is $j = j + S_1 + K_1 = 3 + 1 + 255 \pmod{256} = 3$; this leaves S:

i	0	1	2	3	4	5	6	7	...
S[i]	3	0	2	1	4	5	6	7	...

The $i = 2$ step is $j = j + S_2 + K_2 = 5 + V \pmod{256} = 3$; this leaves S:

i	0	1	2	3	4	...	5+V	...	...
S[i]	3	0	5+V	1	4	...	2	...	...

Finally, at $i = 3$ step is $j = j + S_3 + K_3 = 5 + V + S_3 + k + 3 \pmod{256} = 6 + V + K_3$; this leaves S:

i	0	1	2	3	4	...	5+V	...	6+V+K[3]	...
S[i]	3	0	5+V	6+V+K[3]	4	...	2	...	1	...

$Stream[0] = S[3] = 6 + V + K_3$ if initialization stops here. Attack works if $S[0], S[1], S[2]$ don't change. The probability of this is $\frac{253}{256}^{255} \approx .0513$.

$\Delta^{\otimes} X = X \otimes X^{-1}$. $r-$round characteristic: sequence of differences $\langle \alpha_0, \alpha_1, \ldots, \alpha_r \rangle$. **Definition (Lai):** An iterated cipher is called a Markov cipher if $Pr(\Delta C_1 = \beta | \Delta C_0 = \alpha, C_0 = \gamma)$ is independent of $\gamma, \forall \alpha, \beta \neq e$. *Homogeneous Markov Chain:* $Pr(v_{i+1} | v_i = \alpha)$ is independent of $i, \forall \alpha, \beta$.

Theorem: If an $r-$round iterated cipher is a Markov and the r round keys are independent and uniformly distributed then $\Delta P = \Delta C_0, \Delta C_1, \ldots, \Delta C_r$ is a homogeneous Markov chain and $Pr(\Delta C_s = \alpha_s | \ldots | \Delta C_1 = \alpha_1 | \Delta P = \alpha_0) = \prod Pr(\Delta C_i | \Delta C_{i-1})$.

Definitions: Let $P = (p_{ij})$ be the transition probabilities of a homogeneous Markov chain and ${p_{ij}}^s$ is the probability that state j can be reached from state i in s steps. A Markov chain is *ergodic* if it is aperiodic and irreducible. If a random cipher is selected from Σ_{2^n}, $Pr(P \text{ is ergodic }) \to 1$.

Theorem (OConner): Most Feistel ciphers are resistant to differential attack. Let p_g be the probability of the best linear approximation of g. $|p_g - \frac{1}{2}| = max_k(max_{\alpha \neq 0 \neq \beta} | Pr_x(g(x,h) \cdot \beta = x \cdot \alpha) - \frac{1}{2}|)$ and the best s round linear approximation satisfies $|p_L - \frac{1}{2}|^2 \leq |p_g - \frac{1}{2}|^2$. For DES, $s \geq 4$, $|p_L - \frac{1}{2}|^2 \leq 8|p_f - \frac{1}{2}|^4$.

Definitions: An $r-$round iterated $2m$ bit block cipher with r-round keys each has n bits. A *strong key schedule* is one in which (1) For any s bits of the r round keys derived from k where $s < rn$, it is "hard" to find any of the remaining $rn - s$ bits from the s bits, (2) given a relation between two different master keys, is it "hard" to predict the relationship between any of the round keys. $\langle RK_l \rangle = nMSB(E_{k_i}(IV \oplus l))$.

3.7 New Ciphers

3.7.1 AES-Rijndael

Arithmetic in $GF(2^8)$ with minimum polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$. If $m(\theta) = 0$, matrix for multiplication by θ over $GF(2)$ is denoted by T and squaring by S, then

$$T = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, S = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$Tr(a) = a + a^p + a^{p^2} + \ldots + a^{p^{d-1}}$ and $N(a) = aa^p a^{p^2} \ldots a^{p^{d-1}}$. Linearized polynomial: $L(x) = a_0 x + a_1 x^p + a_2 x^{p^2} + \ldots + a_{d-1} x^{p^{d-1}}$; linear functions can be expressed as linearized polynomials.

Rijndael input: p consisting of Nb words, k with Nk words. State: 4 rows, Nb columns. Key: 4 rows, Nk columns. Both key rows are filled in the following order: Fill leftmost column $s_{i,0}, i = 0, 1, 2, 3$, then next column, etc.

```
    Nb/Nk  4   6   8
       4  10  12  14
       6  12  12  14
       8  14  14  14

Rijndael(p, k, Nb, Nk)  {
    ComputeRoundKeys(K, W[i])
    state= p
    AddRoundKey(state)
    for (i=0, i<Nr, i++) {
         for each byte, b in state, ByteSub(b)
         ShiftRow(state)
         if(i<Nr-1)
             MixCol(state)
         AddRoundKey(state)
         }
}

ByteSub(b) {
    t= 0
    if b!=0 {
        t= 1/b;
    // M= circ(1,0,0,0,1,1,1,1)
    // [Shift right going down].
    // a= (1,1,0,0,0,1,1,0)^T.
    return(Mt + a);
    }

ShiftRow(state) {
    shift right row 1 by 0.
    shift right row 2 by 1.
    shift right row 3 by 2 if Nb<8,
                      3 otherwise.
    shift right row 4 by 3 if Nb<8,
                      4 otherwise.
    }

MixCol(state) {
    multiply each col of state by
             c(x) (mod  x**4+1);
    // c(x)= 0x03x**3+0x01x**2+0x01x+0x02
    // d(x)= 0x0bx**3+0x0dx**2+0x09x+0x0e
    }

AddRoundKey(state) {
    state= state + W[i];
    }

ComputeRoundKeys(K[4*Nk], W[Nb*(Nr+1)]) {
    for(i=0; i<Nk; i++)
```

```
        W[i]= (K[4i], K[4i+1],
               K[4i+2], K[4i+3])
    for(i=Nk; i<Nb*(Nr+1)); i++) {
        t= W[i-1];
        if((i mod Nk)==0)
           t= SubByte(RotByte(t))^RCon(i/Nk);
        if((i mod Nk)==4 and Nk>6)
           t=SubByte(t);
        W[i]= W[i-Nk] ^ t;
        }
    }
```

```
SubByte(w) {
    w= ByteSub(w);
    }

RotByte(w= (a,b,c,d)) {
    w= (b,c,d,a);
    }

RCon[i]= (RC[i], 0x00, 0x00, 0x00);
RC[1]= 0x01;
RC[i+1]=  RC[i]*x (x in poly over GF(2));
```

Note $[ShiftRow, MixCol] = 1$. Rounds Key: $K_{r,0}, K_{r,1}, \ldots, K_{r,15}$. First Round is input key. For $s = r+1$, $T_0 = S[K_{r,13}] + \theta^r$, $T_1 = S[K_{r,14}]$, $T_2 = S[K_{r,15}]$, $T_3 = S[K_{r,12}]$ and $K_{s,i} = K_{r,i} + T_i, 0 \leq i \leq 3$, $K_{s,i} = K_{r,i} + K_{s,i-4}, 4 \leq i \leq 15$. Note that key expansion is equivalent to: $W[i] = W[i-1] \oplus W[i-4]$, if $i \neq 0 \pmod 4$ $W[i] = T(W[i-1]) \oplus W[i-4]$, if $i = 0 \pmod 4$ where $T(a,b,c,d) = (SB(b) \oplus r(i), SB(c), SB(d), SB(a)), r(i) = 0x02^{\frac{i-4}{4}}$ in $GF(2^8)$. Inverse provides linear/differential immunity, linear diffusion provides algebraic complexity.

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} y_7 \\ y_6 \\ y_5 \\ y_4 \\ y_3 \\ y_2 \\ y_1 \\ y_0 \end{pmatrix} = L \begin{pmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{pmatrix}$$

$S[w] = L[w^{(-1)}] + 0x63$. Combined RowShift, ColumnMix and Diffusion and AddRound is $x \mapsto Mx + 0x63 + k_i$ where M is a 16×16 matrix and $min_M(x) = (x+1)^{15})|(x^{16}+1)$ which can be transformed into $P^{-1}MP = V_1 \oplus \ldots \oplus V_{15}$ with $dim(V_i) = (16, 14^3, 10^3, 8^2, 6, 4, 4^4, 2)$.

AES Design Overview: *Linear cryptanalysis resistance for AES design* is provided if no linear trail has a correlation coefficient $> 2^{\frac{n}{2}}$. *Differential cryptanalysis resistance* is provided if there is no differential trail with prop ratio $> 2^{1-n}$. The *prop ratio* of differential trail is approximately the product of the prop ratios of its active S-boxes. The *correlation* of a linear trail is approximately the product of the I/O correlations of its active S-boxes. The *wide trail* strategy is: (1) choose an S-box with maximum prop ratio and correlation $\approx 2^{-6}, 2^{-3}$, respectively; (b) construct diffusion layer in such a way that there are no multiple round trails with few active S-boxes.

Theorem: The weight of a two round trail with Q active columns at the input and output is $\geq 5Q$; The minimum number of active S-boxes in a four round differential or linear trail is 25.

3.7.2 Tea, TwoFish

```
Tea(unsigned K[4], ref unsigned L, ref unsigned R) {
    unsigned d= 0x9e3779b9;
```

```
unsigned s= 0;
for(int i=0; i<32;i++) {
    s+= d;
    L+= ((R<<4)+K[0])^(R+s)^((R>>5)+K[1]);
    R+= ((L<<4)+K[2])^(L+s)^((L>>5)+K[3]);
    }
}
```

(1) 4 different 8×8 bijective, key dependent S boxes. (2) MDS code. (3) PHT: $a' = a + b \pmod{2^{32}}$, $b' = a + 2b \pmod{2^{32}}$. Basic algorithm: whiten, 16 rounds, whiten.

$$MDS = \begin{pmatrix} 0x01 & 0xef & 0x5b & 0x5b \\ 0x5b & 0xef & 0x5b & 0x01 \\ 0xef & 0x5b & 0x01 & 0xef \\ 0xef & 0x01 & 0xef & 0x5b \end{pmatrix}$$

$Round(w_1, w_2, w_3, w_4, k_1, k_2) = (w_1', w_2', w_1, w_2)$: $w_1' = w_3 + F_1(w_1, w_2, r) >>> 1$; $w_2' = (w_4 <<< 1) + F_1(w_1, w_2, r)$; $F_r(w, v) = PHT(g(w), g(v <<< 8)) + k_r \pmod{2^{32}}$; $g(x, y, z, w) = MDS \begin{pmatrix} S_1(x) \\ S_2(y) \\ S_3(z) \\ S_4(w) \end{pmatrix}$. All calculations over $GF(2^8)$.

3.7.3 Miscellaneous

Cramer-Shoup: $G = \mathbb{Z}_p$, $G = \langle g \rangle = \langle g' \rangle$, H, a collision resistant hash whose image is ${\mathbb{Z}_p}^*$. $PK = (G, g, g', h, k, k')$, s, t, t', u, u' randomly selected. $h = sg$, $k = tg + t'g'$, $k' = ug + u'g'$. Encrypt (m): Choose r, random, set $n = H(rg|rg'|m + rnk')$. $E(m) = (x, y, z, w) = (rg, rg', m + rh, rk + rnk')$. Decryption: $D(x, y, z, w)$, check that $(nu + t)x + (nu' + t'))y = w$. If so, compute $z - sx$.

Bit Commitment and coin flips: $b, b' \in \{0, 1\}$. Alice sends Bob $c = commit(b)$, Bob sends Alice b', Alice sends Bob $reveal(c)$. Result is $b \oplus b'$.

Zero Knowledge using 3 color: For each round, Prover randomly permutes colors and *commits* color at each vertex. For each round, Verifier asks to *reveal* color at the vertices of an edge. blob: commit with equality.

Shalevi-Micali Commit: h is a one way function like $SHA1$. $commit(m) = h(r||m)$, r, random. p a 161 bit prime. Pick a, b: $ax + b = z \pmod{p}$, $y = h(x), c = (y, a, b)$. $reveal(c) = x, m$.

Time memory tradeoff: Fix a plaintext block, P and pick $SP_i, i = 1, 2, \ldots, m$. For each i, set $K_0^i = SP_i$ and $K_{j+1}^i = F(E(K_j^i, P)), j = 0, 1, \ldots, t-1$ where F is a randomizing function to avoid short cycles and put $EP_i = K_t^i$. For each i, store (SP_i, EP_i). Phase 2: Get $C = E(P, K)$ from oracle where K is unknown. Compute $X_0 = C$, $X_{i+1} = E(P, X_i)$ until $X_i = EP_j$ for some i, j. Then compute $Y_0 = EP_j$ and $Y_{j+1} = E(P, Y_j)$ until $Y_k = C$ then $K = Y_{k-1}$. If m is the number of starting points for each F, t is the number of encryptions per chain and r is the number of tables. Attack requires mr memory and tr time with the probability of success $1 - e^{-\frac{trm}{k}}$.

Nostradamus ("herding") attack: Let h be a Merkle-Damgard hash with compression function f and

initial value IV. Goal is to hash a prefix value (P) quickly by appending random suffixes (S). Procedure Phase 1: Pick k and generate 2^k random values d_{0i} from each pair of the values $f(IV||d_{i,i+1})$ find two messages $M_{0,j}, M_{1,j}$ which collide under f and call this value $d_{1,j}$ this takes effort $2^{n/2}$ for each pair. Keep doing this (colliding $d_{i,j}, d_{i+1,j}$ under $M_{i,j}, M_{i+1,j}$ to produce $d_{i,j+1}$ until you reach $d_{2^k,0}$. This is the diamond. Publish $y = w(d_{2^k,0})$ where w is the final transformation in the hash as the hash (i.e. - claim $y = h(P||S)$. The cost of phase 1 is $(2^k - 1)2^{n/2}$. In phase 2, guess S' and compute $T = f(IV||P||S')$; keep guessing until T is one of the d_{ij}. Once you get a collision, follow a path through the M_{ij} to $d_{2^k,0}$, append these M_{ij} to $P||S'$ and apply w to get right hash.

3.8 Cryptographic Hashes

Weak collision resistance: Given x, it is computationally infeasible to find $x' \neq x$ with $h(x) = h(x')$. **Strong collision resistance:** It is computationally infeasible to find $x' \neq x$ with $h(x) = h(x')$ for any x, x'. **One-way:** Given a digest z, it is computationally infeasible to find x with $h(x) = z$. Strongly collision resistant implies one-way.

Merkle Damgard construction: $z_0 = IV, z_{i+1} = f(z_i, m_i), h(m) = g(z_r)$, where f is a compression function, r is the number of rounds and $m = m_1||m_2||\ldots||m_r$. If f is collision resistant then so is h. **Hash from Block Cipher:** $m = m_1||m_2||\ldots||m_r$, $H_0 = IV$, $H_i = E_{m_i}(H_{i-1}) \oplus H_{i-1}$, $H(m) = f(H_i)$. is the Meyer-Davis construction.
$g_i = e_{g_{i-1}}(x_i) + x_i$, $g_i = e_{g_{i-1}}(x_i) + x_i + g_{i-1}$, $g_i = e_{g_{i-1}}(g_{i-1} + x_i) + x_i$, $g_i = e_{g_{i-1}}(g_{i-1} + x_i) + g_{i-1} + x_i$.

Chaum Hash: α, β two primitive elements of $\mathbb{Z}_p$, $h(x, y) = \alpha^x \beta^y \pmod p$. If there's a collision, $log_\alpha(\beta)$ can be computed efficiently. $h(0^{t+1}||y_1)$, $g_{i+1} = h(g_i||1||y_{i+1})$. Do reduction proof.

Iterative construction is vulnerable to multi-collision (Joux): Suppose $M_1, M_1'; M_2, M_2'; \ldots; M_t, M_t'$ all collide. From these we get 2^t collisions. If r people each have one of N possible birthdays, there is a greater than .5 chance of k collisions if $r > N^{\frac{k-1}{k}}$. Prove this fact.

Random Oracle Model: Let f be a OWF with trapdoor, $(y_1, y_2) = (f(r), h(r) + m)$ is used as encryption. An oracle with l requests L, $Pr(guess\ right) = P(r \in L) + \frac{1}{2}P(\neg r \in L)$. Set $p = \frac{1}{2} + e$, $e \leq Pr(r \in L)$. Canetti, Goldreich, Halevi constructed a cryptosystem that is secure in Random Oracle Model but insecure for any concrete hash.

MD-4: In description below, K[0]= 0, K[1]= 0x5a827999, K[2]= 0x6ed9eba1. $F(A, B, C) = (A \wedge B) \vee (\neg A \wedge C)$, $G(A, B, C) = (A \wedge B) \vee (A \wedge C) \vee (B \wedge C)$, $H(A, B, C) = (A \oplus B) \oplus C$. $W_i = X_{\sigma(i)}, i = 0, 1, \ldots, 47$. $Q_{-4} = A$, $Q_{-3} = D$, $Q_{-2} = C$, $Q_{-1} = B$. $Q_i(A, B, C) = (Q_{i-4} + F(Q_{i-1}, Q_{i-2}, Q_{i-3}) + W_i + K_0) <<< s_i, 0 \leq i \leq 15$, $Q_i(A, B, C) = (Q_{i-4} + G(Q_{i-1}, Q_{i-2}, Q_{i-3}) + W_i + K_1) <<< s_i, 16 \leq i \leq 31$, $Q_i(A, B, C) = (Q_{i-4} + H(Q_{i-1}, Q_{i-2}, Q_{i-3}) + W_i + K_2) <<< s_i, 32 \leq i \leq 47$.

```
MD-4(Y[0] , ..., Y[N-1])
    K[0]= 0; K[1]= 0x5a827999; K[2]= 0x6ed9eba1;
    (A, B, C, D)= (0x67452301, 0xefcdab89, 0x98badcfe, 0x10325476);
    for(i=0; i<(N/16); i++) {
        X[j]= Y[16i+j], j= 0, 1, ..., 15;
        W[j]= X[SIGMA(j)], j= 0, 1, ..., 47;
        Q[-4]= A;
        Q[-3]= D;
```

```
        Q[-2]= C;
        Q[-1]= B;
        // Calculate Q[i] recursively according to formula above
        (A, B, C, D)+= (Q[44], Q[45], Q[46], Q[47]);
        (A, B, C, D)= (A, D, C, B);
        }
    return (A, B, C, D);
```

Dobbertin attack on MD4, steps 20-35 Let M and M' be 512 bit messages consisting of 16, 32-bit works $X_0, X_1, \ldots, X_{15}$ with $X_i = X'_i$ for all i except $i = 12$ and let $X'_{12} = X_{12} + 1 \pmod{2^{32}}$. We want to find a collision. $\Delta_i = (Q'_j - Q_j, Q'_{j-1} - Q_{j-1}, Q'_{j-2} - Q_{j-2}, Q'_{j-3} - Q_{j-3})$ after step i. Dobbertin attack consists of three steps: (1) Show that if $\Delta_{19} = (0, 2^{25}, -2^5, 0)$ then $\Delta_{35} = (0, 0, 0, 0)$ with probability $p > 2^{-30}$ (actually, $p > 2^{-22}$); (2) get conditions on M (i.e. on the X_i) based on round 12, that guarantee $\Delta_{19} = (0, 2^{25}, -2^5, 0)$; (3) find $X_0, X_1, \ldots, X_{11}$ that produce candidates that present the desired conditions at step 12, after about 2^{22} of these, you'll get a collision. The work factor is about 2^{20}.

1. Steps 19-35. Suppose $\Delta_{19} = (0, 2^{25}, -2^5, 0)$ and $G(Q_{19}, Q_{18}, Q_{17}) = G(Q'_{19}, Q'_{18}, Q'_{17})$, then the following table holds:

j	$\Delta(Q_j)$	$\Delta(Q_{j-1})$	$\Delta(Q_{j-2})$	$\Delta(Q_{j-3})$	i	s_j	p	In
19	2^{25}	-2^5	0	0	$*$	$*$	$*$	$*$
20	0	2^{25}	-2^5	0	1	3	1	X_1
21	0	0	2^{25}	-2^5	1	5	$\frac{1}{9}$	X_5
22	-2^{14}	0	0	2^{25}	1	9	$\frac{1}{3}$	X_9
23	2^6	-2^{14}	0	0	1	13	$\frac{1}{3}$	X_{13}
24	0	2^6	-2^{14}	0	1	3	$\frac{1}{9}$	X_2
25	0	0	2^6	-2^{14}	1	5	$\frac{1}{9}$	X_6
26	-2^{23}	0	0	2^6	1	9	$\frac{1}{3}$	X_{10}
27	2^{19}	-2^{23}	0	0	1	13	$\frac{1}{3}$	X_{14}
28	0	2^{19}	-2^{23}	0	1	3	$\frac{1}{9}$	X_3
29	0	0	2^{19}	-2^{23}	1	5	$\frac{1}{9}$	X_7
30	-1	0	0	2^{19}	1	9	$\frac{1}{3}$	X_{11}
31	1	-1	0	0	1	13	$\frac{1}{3}$	X_{15}
32	0	1	-1	0	2	3	$\frac{1}{3}$	X_0
33	0	0	1	-1	2	9	$\frac{1}{3}$	X_8
34	0	0	0	1	2	11	$\frac{1}{3}$	X_4
35	0	0	0	0	2	15	1	$X_{12}, X_{12} + 1$

Steps 12 to 19. To get $\Delta_{19} = (0, 2^{25}, -2^5, 0)$, $Q_{16} = Q'_{16}$, $Q_{19} = Q'_{19} + 2^{25}$, $Q_{18} + 2^5 = Q'_{18}$, $Q_{17} = Q'_{17}$ and $Q_i = Q'_i, 8 \leq i \leq 11$.

j	i	M In	M' In
12	0	X_{12}	$X_{12} + 1$
13	0	X_{13}	X_{13}
14	0	X_{14}	X_{14}
15	0	X_{15}	X_{15}
16	1	X_0	X_0
17	1	X_4	X_4
18	1	X_1	X_8
19	1	X_{12}	$X_{12} + 1$

These yield the following conditions: $(Q'_{12} <<< 29) - (Q_{12} <<< 29) = 1$, $F(Q'_{12}, Q_{11}, Q_{10}) - F(Q_{12}, Q_{11}, Q_{10}) = (Q'_{13} <<< 25) - (Q_{13} <<< 25)$, $F(Q'_{13}, Q_{12}, Q_{11}) - F(Q_{13}, Q_{12}, Q_{11}) = (Q'_{14} <<< 21) - (Q_{14} <<< 21)$, $F(Q'_{14}, Q_{13}, Q_{12}) - F(Q_{14}, Q_{13}, Q_{12}) = (Q'_{15} <<< 13) - (Q_{15} <<< 13)$, $G(Q'_{15}, Q'_{14}, Q_{13}) - G(Q_{15}, Q_{14}, Q_{13}) = Q_{12} - (Q'_{12},\ G(Q'_{16}, Q'_{15}, Q_{14}) - G(Q_{16}, Q_{15}, Q_{13}) = Q_{13} - (Q'_{13},\ G(Q'_{17}, Q'_{16}, Q_{15}) - G(Q_{17}, Q_{16}, Q_{14}) = Q_{12} - Q'_{12} + (Q_{18} <<< 23) - (Q_{18} <<< 23)'$, $G(Q'_{18}, Q'_{17}, Q_{16}) - G(Q_{18}, Q_{17}, Q_{15}) = Q_{15} - Q'_{15} + (Q_{19} <<< 19) - (Q_{19} <<< 19)'$). Choose $Q_{14}, Q_{15}, \ldots, Q_{19}$ arbitrarily and solve for $Q_{10}, Q_{13}, Q'_{13}, Q'_{14}, Q'_{15}$, use the Q's to solve for $X_j, j = 0, 4, 8, 12, 13, 14, 15$. For the solutions,

$$(Q_{10}, Q_{11}, Q_{12}, Q_{13}, Q_{14}, Q_{15}, Q_{16}, Q_{17}, Q_{18}, Q_{19}, Q'_{12}, Q'_{13}, Q'_{14}, Q'_{15}),$$

Δ_{19} will hold if $X_{13} =$ *anything*, $X_{14} = (Q_{14} <<< 21) - Q_{10} - F(Q_{13}, Q_{12}, Q_{11})$, $X_{15} = (Q_{15} <<< 13) - Q_{11} - F(Q_{14}, Q_{13}, Q_{12})$, $X_0 = (Q_{16} <<< 29) - Q_{12} - G(Q_{15}, Q_{14}, Q_{13}) - K_1$, $X_4 = (Q_{17} <<< 27) - Q_{13} - G(Q_{16}, Q_{15}, Q_{14}) - K_1$, $X_8 = (Q_{18} <<< 23) - Q_{14} - G(Q_{17}, Q_{16}, Q_{15}) - K_1$, $X_{12} = (Q_{19} <<< 19) - Q_{15} - G(Q_{18}, Q_{17}, Q_{16}) - K_1$, $Q_9 = (Q_{13} <<< 25) - F(Q_{12}, Q_{11}, Q_{10}) - X_{13}$, $Q_8 = (Q_{12} <<< 19) - F(Q_{11}, Q_{10}, Q_{09}) - X_{12}$. Can choose $Q_{12} = -1$, $Q'_{12} = 0$, $Q_{11} = 0$ to simplify. This means we can pick $Q_{14}, Q_{15}, Q_{16}, Q_{17}, Q_{18}, Q_{19}$ arbitrarily and determine $Q_{10}, Q_{13}, Q'_{13}, Q'_{14}, Q'_{15}$ subject to the checks $G(Q_{15}, Q_{14}, Q_{13}) - G(Q'_{15}, Q'_{14}, Q'_{13}) = 1$ and $F(Q'_{14}, Q'_{13}, 0) - F(Q_{14}, Q_{13}, -1) - (Q'_{15} <<< 13) + (Q_{15} <<< 13) = 0$. Finally, we must insure the solutions is admissible by checking that $G(Q'_{19}, Q'_{18}, Q_{17}) = G(Q_{19}, Q_{18}, Q_{17})$. Under these circumstances the solution is a candidate for the differential. Once one candidate is found use the "continuity" of F and G by modifying one bit of the candidate at a time, the continuity makes it likely this will work.

Steps 0 to 11. Having found Q_8, Q_9, Q_{10}, Q_{11} such that

$$MD4_{12,\ldots,47}(Q_8, Q_9, Q_{10}, Q_{11}, X) = MD4_{12,\ldots,47}(Q_8, Q_9, Q_{10}, Q_{11}, X')$$

we need to find $MD4_{0,\ldots,11}(IV, X) = (Q_{11}, Q_{10}, Q_9, Q_8)$. We are free to choose $X_j, j = 1, 2, 5, 6, 7, 9, 10, 11$. We pick X_1, X_2, X_3, X_5 at random and compute $X_6, X_7, X_9, X_{10}, X_{11}$ such that $MD4_{6,\ldots,11}(Q_2, Q_3, Q_4, Q_5, X) = (Q_{11}, Q_{10}, Q_9, Q_8)$. Since $Q_{11} = (Q_7 + F(Q_{10}, Q_9, Q_8) + X_{11}) <<< 19$, if can do this by making $X_{11} = (Q_{11} <<< 13) - Q_7 - F(Q_{10}, Q_9, Q_8)$ and similarly for X_{10}, X_9. We can't do this for X_9 but since $Q_8 = (Q_4 + F(Q_7, Q_6, Q_5) + X_8) <<< 3$, if $Q_7 = -1, Q_6 = (Q_8 <<< 29) - Q_4 - X_8$ the desired equation holds for all such X_8; in particular, by picking $X_6 = (Q_6 <<< 21) - Q_2 - F(Q_5, Q_4, Q_3)$ and $X_7 = (Q_7 <<< 13) - Q_3 - F(Q_6, Q_5, Q_4)$. These guarantee $\Delta_{35} = 0$.

SHA1(M,n)
// M is message, n is number of 512 bit blocks

M= SHA1Pad(M)
$f_i(B, C, D) = (B \wedge C) \vee (\overline{B} \wedge D), 0 \le i \le 19$
$f_i(B, C, D) = (B \oplus C \oplus D), 20 \le i \le 39$
$f_i(B, C, D) = (B \wedge C) \vee (B \wedge D) \vee (C \wedge D), 40 \le i \le 59$
$f_i(B, C, D) = (B \oplus C \oplus D), 60 \le i \le 79$

$K_i = 0x5a827999, 0 \le i \le 19; K_i = 0x6ed9eba1, 20 \le i \le 39$
$K_i = 0x8f1bbcdc, 40 \le i \le 59; K_i = 0xca62c1d6, 60 \le i \le 79$

$H_0 = 0x67452301, H_1 = 0xefcdab89, H_2 = 0x98badcfe, H_3 = 0x10324576, H_4 = 0xc3d2e1f0$

for (i=0, $i < n$, i++) {
$M_i = W_0 || W_1 || \ldots || W_{15}$
for($j = 16, j < 80, j++$) {

// $ROTL^1$ below is difference between SHA-0 and SHA-1
$W_j = ROTL^1(W_{j-3} \oplus W_{j-8} \oplus W_{j-14} \oplus W_{j-16})$
}
$A = H_0, B = H_1, C = H_2, D = H_3, E = H_4$
for($j = 0, j < 80$; j++) {
$ROTL^5$ below is correlated to lowest wt differential
$t = ROTL^5(A) + f_j(B, C, D) + E + W_j + K_j$
$E = D, D = C, C = ROTL^{30}(B), B = A, A = t$
}
$H_0 += A, H_1 += B, H_2 += C, H_3 += D, H_4 += E$
}

```
SHA-1Pad(x)   // with MD strengthening
    Append 1 and enough 0's until there are 64 bits remaining
    Append size hashed in 64 bit format
    return(x)
```

Shamir's non-linear functions with maximal period: $x \to x^2 \wedge c$, $x \to x + 4h(x) + 1$. *Example:* $x \to (x+1)(2x+1)$.

SHA-3 (Keccak): Basic mixing function is $Keccak - f[b]$. $b = r + c$. $b = 25, 50, 100, 200, 400, 800, 1600$. For SHA-3, $r = 1024$, $c = 576$, $b = 1600$. $w = \frac{b}{25} = 2^l$, $n_r = 12 + 2l$. So for SHA-3, $n_r = 24$. State $s[b]$ is addressed by $a(x, y, z) = w(5y + x) + z$, little endian. Terminology: row, constant (y, z), column, constant (x, z), lane, constant (x, y). Pad: 10^*1.

```
Keccak-f[r,c](A, RC)
    for(i=0;i<nr;i++)
        A= Round[b](A,RC);

rot(W,r)
    W[(i+r)(mod laneSize)]= W[i];

Round[b](A, RC)
    C[x]= A[x,0]^A[x,1]^A[x,2]^A[x,3]^A[x,4];
    D[x]= C[x-1]^rot(C[x+1], 1);
    A[x,y]= A[x,y]^D[x];
    B[y,2x+3y]= rot(A[x,y], r(x,y));
    A[x,y]= B[x,y]^(NOT(A[x,y]) AND B[x+2,y]);
    A[0,0]= A[0,0]^RC;

    r(x,y)  x=3  x=4  x=0  x=1  x=2
    y=2      25   39    3   10   43
    y=1      55   20   36   44    6
    y=0      28   27    0    1   62
    y=4      56   14   18    2   61
    y=3      21    8   41   45   15

Keccak-f[r,c](M)
    P=M||(0x01 0x00 ... 0x00;
    P^=   0x80;
    s[i,j]= 0;

Absorb(P[i])
    s[x,y]^= P[i][x+5y];
    s= Keccak-f[r,c]

Squeeze(k)
    first k bits of s
```

$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$. $rc[t] = x^t \pmod{x^8 + x^6 + x^5 + x^4 + 1}$, $RC[i_r][0, 0][2^j - 1] = rc[j + 7i_r], 0 \leq j < l$. Distinguisher: $2^{\frac{b}{2}}$. Inner collision: $n^2 2^{-(c+1)}$. State recovery: $nm2^{-c}$.

Changes from MD4 to MD5: (1) 64 steps, function for final 16 rounds is $I(A, B, C) = B \oplus (A \vee \neg C)$, (2)

$G(A,B,C) = (A \wedge C) \vee (B \wedge \neg C)$, (3) each round uses different constant, (4) each step adds result of previous step, (5) the order of input words to the steps is different,(6) shift values are different. Chinese attack uses "precise" differential (signed difference) where 0 indicates no difference, + indicates $1 \rightarrow 0$ difference and − indicates $0 \rightarrow 1$ difference. This is different from both xor and modular difference; for example, if $z' = 10100101, z = 10010101$, $\nabla(z', z) = 00 + -0000$.

Chinese attack on MD5. Attack proceeds in four phases: (1) specify input differential patters via modular difference (hard and "done by hand" according to Wang), (2) specify output differential pattern (only 1 known) that is easily satisfied in earlier rounds, (3) derive sufficient conditions propagation; (4) generate pairs of 1024 bit numbers that satisfy 3 (deterministically when possible). To do step 4: (a) generate M_0 at random; (b) use single step modification to M_0 to satisfy sufficient conditions; (c) use multi-step modifications to insure conditions hold in middle rounds; (d) check conditions for all remaining steps; (e-f) do the same for M_1; compute $M_0' = M_0 + \Delta M_0$ and $M_1' = M_1 + \Delta M_1$ according to the input differential. **Conditions:** $T_j = F(Q_{j-1}, Q_{j-2}, Q_{j-3}) + Q_{j-4} + K_j + W_j$, $R_j = T_j <<< s_j$, $Q_j = Q_{j-1} + R_j$, now apply modular difference and derive conditions on ΔT_j and ΔQ_j for differential (below) to hold.

$\Delta X = X' - X$. $\Delta H_0 \rightarrow_{(M_0, M_0')} \Delta H_1 \rightarrow_{(M_1, M_1')} \Delta H_2 \ldots \rightarrow_{(M_{i-1}, M_{i-1}')} \Delta H_i = H$ with each composed of $\Delta H_i \rightarrow_{P_2} \Delta R_{i+1,1} \rightarrow_{P_2} \Delta R_{i+1,2} \rightarrow_{P_3} \Delta R_{i+1,3} \rightarrow_{P_4} \Delta R_{i+1,4} = \Delta H_{i+1}$. Let $\Delta i, j = x'_{i,j} - x_{i,j} = \pm 1$ and $\Delta x_i[j_1, j_2, \ldots, j_l] = x_i[j_1, j_2, \ldots, j_l] - x_i$. Collision is caused by 1024 bit input: (M_0, M_1) with $\Delta M_0 = (0,0,0,0,2^{31},0,0,0,0,0,0,2^{15},0,0,2^{31},0)$ and $\Delta M_1 = (0,0,0,0,2^{31},0,0,0,0,0,0,-2^{15},0,0,2^{31},0)$. Sufficient conditions insure that differential holds with high probability. At 8th iteration, $b_2 = c_2 + (b_1 + F(c_2, d_2, a_2) + m_7 + t_7) <<< 22$, we try to control $(\Delta c_2, \Delta d_2, \Delta a_2, \Delta b_1) \rightarrow \Delta b_2$ with the following (A) non-zero bits of Δb_2: $d_{2,11} = 1, b_{2,1} = 0$, $d_{2,26} = \overline{a_{2,26}} = 1, b_{2,16} = 0$, $d_{2,28} = \overline{a_{2,28}} = 0, b_{2,i} = 0$, $d_{2,11} = 1, b_{2,24} = 0$; (B) zero bits of Δb_2: $c_{2,i} = 0$, $d_{2,i} = a_{2,i}$, $c_{2,1} = 1$, $d_{2,6} = \overline{a_{2,6}} = 0$, $d_{2,i} = 0$, $d_{2,12} = 1$, $a_{2,24} = 0$, 7th bit of c_2, d_2, a_2 result in no change in b_2. Algorithm 1: Repeat until first block is found (a) Select random M_0, (b) Modify M_0, (c) $M_0, M_0' = M_0 + \Delta M_0$ produce $\Delta M_0 \rightarrow (\Delta H_1, \Delta M_1)$ with probability 2^{-37}, (d) Test characteristics. 2: Repeat until first block is found (a) Select random M_1, (b) Modify M_1, (c) $M_1, M_1' = M_1 + \Delta M_1$ produce $\Delta M_1 \rightarrow 0$ with probability 2^{-30}, (d) Test characteristics.

Comments from NIST: Randomization (prevent offline computation for herding): $RMX(r, M_1 | \ldots | M_L) = (r | m_1 \oplus r | \ldots | m_L \oplus r)$. $H_r(M_1 | \ldots | M_L) = H(r | m_1 \oplus r | \ldots | m_L \oplus r)$. Transmit r. Herding attack: first committing to an output h, then mapping messages with arbitrary starting values to h. Joux: If H_1, H_2 are n bit hashes; $H_1(M) || H_2(M)$ can be broken in $O(n 2^{\frac{n}{2}})$. *Haifa:* $h_{i+1} = CF(h_i, M_i, bitlength, salt)$.

Joux attack on SHA-0: Idea is to linearize by replacing + with $\oplus$, as well as replacing MAJ and IF with $\oplus$. This is "SHI-1." Now select the collision in two steps. First, ignoring message expansion a 5-round correction for a local collision is: $\delta = W_1^{(i)} \oplus W_2^{(i)}$, $\delta = ROL^5(W_1^{(i+1)} \oplus W_2^{(i+1)})$, $\delta = W_1^{(i+2)} \oplus W_2^{(i+2)}$, $\delta = ROL^{30}(W_1^{(i+3)} \oplus W_2^{(i+3)})$, $\delta = ROL^{30}(W_1^{(i+4)} \oplus W_2^{(i+4)})$, $\delta = ROL^{30}(W_1^{(i+5)} \oplus W_2^{(i+5)})$. Since message expansion reduces the freedom of choice, no changes can be introduced in the last 5 rounds because there is no way to correct them. We focus on expansion patterns in bits $j, j+5, j+30$. For a 5-round correction, about $\frac{1}{32}$ possible ones will work beacuse they follow the message expansion. Now we look at candidate collisions (W, Δ). Taking into account the non-linearized version, we focus on patterns in the high order bit (which has no carries) and can calculate the probability of successful propagations of $1 \rightarrow 1$ and $1 \rightarrow 0$ transitions through MAJ and IF. The strategy is to choose Δ and then find W.

Attack expands by studying "SHI-2" which leaves $\oplus$ in SHI-1 but reintroduces MAJ and IF. Effects of MAJ and IF are separated into four cases: (1) No change in b, c, d (the only bits affecting the f_i; (2) Change in one bit of b; (3) Change in one bit of c or d; (4) Change in one bit of each of c and d. "SHI-3"

takes SHI-1 and reintroduces the (non-linear) add used in calculating a but leaves IF and MAJ's linear replacements. Attack gives a collision in 2^{61}. This was improved by Biham and Chen by introducing "neutral bit" estimates and starting the perturbation later in the rounds.

For SHA-0, change bit 1 (because the + operation is linear in bit 1) which shifts to bit 31 and is linear in $\oplus$. Disturbance bit vector: $(m_0^{(0)}, m_0^{(1)}, \ldots, m_0^{(79)})$. Perturbation mask: $-5 \leq i \leq -1, M_0^{(i)} = 0$, $0 \leq i \leq 79, M_{0,k}^{(i)} = 0$, if $k \neq 1$ $0 \leq i \leq 79, M_{0,1}^{(i)} = M_0^{(i)}$. Corrective masks: $-4 \leq i \leq 79, M_1^{(i)} = ROL_5(M_1^{(i-1)})$, $-3 \leq i \leq 79, M_2^{(i)} = M_1^{(i-2)}$, $-2 \leq i \leq 79, M_3^{(i)} = ROL_{30}(M_1^{(i-3)})$, $-1 \leq i \leq 79, M_3^{(i)} = ROL_{30}(M_1^{(i-4)})$, $0 \leq i \leq 79, M_3^{(i)} = ROL_{30}(M_1^{(i-5)})$.

Early round differentials are prescribed and later round differentials hold with non-negligible probability (2^{-61}, 2^{-56} using *neutral bits* — A bit is neutral if flipping it doesn't change differential pattern). In Wang's multi-block attack: patch final round errors in next block. Early rounds are non-linear and prescribed. Late rounds linear and probabilistic. *Procedure:* Fix linear characteristic, fix non-linear characteristic, modify message (keeping differential) if conflict in mid round.

SHA-256 definitions: $Ch(x,y,z) = (x \wedge y) \oplus (\neg x \wedge z)$, $\psi_{256}^{i,j,k}(x) = ROTR^i(x) \oplus ROTR^j(x) \oplus ROTR^k(x)$, $\Sigma_0^{256}(x) = \psi_{256}^{2,13,22}(x)$, $\sigma_0^{256}(x) = \phi_{256}^{7,18,3}(x)$,
SHA-512 definitions: $Ch(x,y,z) = (x \wedge y) \oplus (\neg x \wedge z)$, $\psi_{512}^{i,j,k}(x) = ROTR^i(x) \oplus ROTR^j(x) \oplus ROTR^k(x)$, $\Sigma_0^{512}(x) = \psi_{512}^{28,34,39}(x)$, $\Sigma_1^{512}(x) = \psi_{512}^{14,18,41}(x)$.
$\sigma_0^{512}(x) = \phi_{512}^{1,8,7}(x)$,

SHA-256$(M_1||M_2||\ldots||M_N)$**:**
for$(i = 1; i \leq N; i++)$ {
$W_t = M_t^{(i)}, 0 \leq t \leq 15$,
$W_t = \sigma_1^{256}(W_{t-2}) \oplus W_{t-7} \oplus \sigma_0^{256}(W_{t-15}) \oplus W_{t-16}, 16 \leq t \leq 63$;
$a = H_0^{(i-1)}$; $b = H_1^{(i-1)}$; $c = H_2^{(i-1)}$; $d = H_3^{(i-1)}$;
$e = H_4^{(i-1)}$; $f = H_5^{(i-1)}$; $g = H_6^{(i-1)}$; $e = H_7^{(i-1)}$;
for$(t = 0; t < 64; t++)$ {
$T_1 = h + \Sigma_1^{256}(e) + Ch(e,f,g) + K_t^{256} + W_t$; $T_2 = \Sigma_0^{256}(a) + Maj(e,f,g)$;
$h = g$; $g = f$; $f = e$; $e = d + T_1$; $d = c$;
$c = b$; $b = a$; $a = T_1 + T_2$;
}
$H_0^{(i)} = a + H_0^{(i-1)}$; $H_1^{(i)} = b + H_1^{(i-1)}$; $H_2^{(i)} = c + H_2^{(i-1)}$; $H_3^{(i)} = d + H_3^{(i-1)}$;
$H_4^{(i)} = e + H_4^{(i-1)}$; $H_5^{(i)} = f + H_5^{(i-1)}$; $H_6^{(i)} = g + H_6^{(i-1)}$; $H_7^{(i)} = h + H_7^{(i-1)}$;
}

SHA-512 is the same except there are 79 rounds and the words are 64 bits long.

Cayley Hashes: Let $S = \{s_0, \ldots, s_{k-1}\} \subseteq G$ and $M = m_1||m_2||\ldots||m_n, m_i \in [0, k-1]$. Define $H_M) = s_{m_1} s_{m_2} \ldots s_{m_n}$. *Representation Problem:* Given G, S, find short $\prod s_i = 1$. *Balence Problem:* Given G, S, find short $\prod s_i = \prod s_i'$. *Factoring Problem:* Given $G, S, g \in G$, find short $\prod s_i = g$.

Example: $p(x) \in \mathbb{Z}_2[x]$, irreducible, $deg(p) = n$, $G = SL_2(F_{2^n})$, $S = \langle \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} x & x+1 \\ 1 & 1 \end{pmatrix} \rangle$ is the Tillich-Zemor scheme. $G = SL_2(p)$, $S = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \rangle$ is the LPS scheme.

3.9 Elliptic Curve Crypto

Definition: $E_F(a,b) : y^2 = x^3 + ax + b$ where $a, b \in F$ and $char(F) \neq 2, 3$; we sometimes write $E_q(a,b)$ if $F = GF(q)$. For ECC, also require smooth; namely, $4a^3 + 27b^2 \neq 0 \pmod p$, $p = char(F)$. For $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ define $P + Q = (x_3, y_3)$ with $x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1$ where $\lambda = \frac{(y_1 - y_2)}{(x_1 - x_2)}$ if $P \neq Q$ and $\lambda = \frac{(3x_1^2 + a)}{(2y_1)}$ if $P = Q$. For $char(F) = 2$, $E_F(a,b) : y^2 + xy = x^3 + ax + b$ and $x_3 = \lambda^2 + \lambda + a + x_1 + x_2, y_3 = \lambda(x_1 + x_3) + x_3 + y_1$ where $\lambda = \frac{(y_1 - y_2)}{(x_1 - x_2)}, P \neq Q$ and $\lambda = x_1 + \frac{y_1}{x_1}, P = Q$.

ECDSA: For an ECC system, the public key parameters are q, a, b, P (P is called the base point); pick $1 < x < p$, x is the private key. Public key is $Q = xP$. *ECDLP:* Find x knowing Q. *ECC Encrypt:* To encrypt m (already an integer in the right range), map it to a point on the curve P_M, pick $1 < k < p$, send $(kP, kQ + P_M)$. *ECC Decrypt:* Receive (L, M) calculate $M - xL = P_M$ and map it back to the integer message. Here is a way to embed integers in curves: For $q = p^r$, odd, select parameter κ so that the probability of failure is $2^{-\kappa}$; m is message and $0 \leq m < M, q > \kappa M$ and $x = m\kappa + j \in F_q$ now for the first j for which $x^3 + ax + b$ is a square, use the corresponding point $P = (x, \sqrt{x})$. *ECDSA sign:* Select k at random, compute $kP, r = f_E(kP), s = k^{-1}(H(M) + xr)$. Signature is (r, s). *ECDSA verify:* $u_1 = s^{-1}H(M), u_2 = s^{-1}r$, accept if $f_E(u_1P + u_2Q) = r$.

Curve selection: Avoid *anomalous curves* (Definition: $char(F) \mid \#E_F(a,b)$), and *supersingular curves* (Definition: $\#E_q(a,b) = q + 1 - t, q \mid t$ — t is Frobenius trace satisfying $(\phi_q)^2 - t\phi_q + q = 0$; also t is $Tr(\phi_q)$), CM 3 ($a = 0, p = 3 \pmod 4$), MOV-vulnerable (Frey-Ruck) For comparison, attacks on DLP: $L(v, c, n) = exp(c(ln(p)^v(ln(ln(p))^{1-v})$, NFS discrete log is $L_n[\frac{1}{3}, (\frac{64}{9})^{\frac{1}{3}}]$. Best known ECDLP is $EC(n) = \sqrt{n}$. In comparisons, usually put $n = lg(\lceil q \rceil), N = lg(\lceil p \rceil)$ and put $\frac{E_{EC}}{E_{CONV}} = \frac{2^{\frac{n}{2}}}{exp(cN^{\frac{1}{3}}(log(N(log(2))^{\frac{2}{3}}}$.

NIST Curves: Use prime fields $\mathbb{F}_p$ with $p = 2^{192} - 2^{64} - 1, 2^{224} - 2^{96} + 1, 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1, 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1, 2^{521} - 1$ or binary fields $\mathbb{F}_q$ with $q = 2^{163}, 2^{233}, 2^{283}, 2^{409}, 2^{571}$. $\#E_p(a,b) = q + 1 - t, |t| \leq 2\sqrt{q}$ and t is called the trace of E. $E_q(a,b)$ has rank 1 or 2, that is: $E_q(a,b) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ and $n_2 \mid n_1, n_2 \mid (q-1)$. If $n_2 = 1, E_q(a,b) \cong \mathbb{Z}_{n_1} = \{kP : 0 < k < n_1\}$ and P is a generator. $E_q(a_1, b_1) \cong E_q(a_2, b_2)$ if $a_1 = u^4 a_2$ and $b_1 = u^4 b_2$. $E_q, q = p^n$ is supersingular if $p \mid t$. Field represented as polynomial or normal basis. Hyperelliptic: higher genus.

Weil-Deligne: Set $\zeta(t, E/F_q) = exp(\sum_r \frac{N_r t^r}{r})$, where N_r is the number of solutions of E/F_{q^r}. $\zeta(t, E) = \frac{a - at + qt^2}{(1-t)(1-qt)}, N_1 = q + 1 - a, N_r = q^r + 1 - \alpha^r - \beta^r$ where α, β are reciprocal roots of the numerator. Random selection of (E, B): Generate x, y, a at random and compute $b = y^2 - (x^3 + ax)$, check there are not multiple roots. To compute $|E|$, use Schoof.

MOV Attack: $E_q(a,b) \mapsto F_{q^k}^*$ if n, the curve order, satisfies $n \mid (q^k - 1)$ then use index calculus, small probability of supersingular or $k \leq log^2(q)$. Attack fails if $k > log^2(q)$ (Frey and Ruck extended the attack).

IBE: Suppose $p = 6q - 1$, $E_p : y^2 = x^3 + 1 \pmod p$ and suppose $\#E = 6q$. $\exists P_0 \neq \infty$ and $qP_0 = \infty$. Finally, suppose there is a bilinear map, $\tilde{e}(P, Q)$, from points into q-th roots of unity that is easy to compute with $\tilde{e}(aP_0, bP_0) = \tilde{e}(P_0, P_0)^{ab}$. $\tilde{e}(P_0, P_0) \neq 0$ and two hash functions: $H_1 : \langle 2^\infty \rangle \to kP_0$ and $H_2 : \{\omega^i\} \to \langle 2^n \rangle$. Pick a secret $s : P_1 = sP_0$. To encrypt to ID: set $D_U = sH_1(ID)$, $g = \tilde{e}(H_1(ID), P_1)$, choose $r \neq 0 \pmod q$ and compute $t = m \oplus H_2(g^r)$, $A \to B : c = (rP_0, t)$. To decrypt: Get (u, v), compute $h = \tilde{e}(H_1(D_u, u)$, $m = v \oplus H_2(h)$. Note $h = g^r$.

ECC Point Operation Costs: I = inverse cost $/GF(p)$. S = square cost $/GF(p)$. M = multiply cost $/GF(p)$.

Operation	Cost	Modular Op	Cost
$2P$	$I+2S+2M$	Add, Sub	$O(lg(n))$
$P+Q$	$I+S+2M$	Multiply	$O(lg(n)^2)$
$2P+Q$	$2I+2S+2M$	Invert	$O(lg(n)^2)$
$P+Q$, $P-Q$	$I+2S+4M$	Exp	$O(lg(n)^3)$

If $X=\langle X_1, X_2, \ldots, X_n\rangle$ and $Y=\langle Y_1, Y_2, \ldots, Y_n\rangle$ then $Pr(\Delta X, \Delta Y)=\frac{1}{2^n}$ for perfect differential resistance. $(\Delta X, \Delta Y)$ is a differential characteristic. $N_D=\frac{c}{p_D}$ and $p_D=\prod_i^{\gamma}\beta_i$ where γ is the number of active boxes.

Definitions: $Tr(x)=x+x^p+\ldots+x^{p^{n-1}}$. e,d is a dual basis if $Tr(d^{(i)}e^{(j)})=\delta(i\oplus j)$.

3.10 Algebraic and other attacks

Hadamard-Walsh: $W_f(w)$, measures distance to affine and completely determines f. The *autocorrelation* is $r_f(w)$ measures differential and does not determine f.

Definitions: *Balanced:* weight is 2^{n-1}. $CI_f(t)$: output is statistically independent on any t input bits. *Resilient:* $R_f(t)$ is $CI_f(t)$ and balanced. *Non-linearity:* N_f is distance to affine. $N_f=min_{g\in RM(1,n)}d(f,g)=2^{n-1}-\frac{1}{2}max_w|W_f(w)|$. $\epsilon=\frac{N_f}{2^n}-\frac{1}{2}$ *Linearity:* $L_f=max_w|W_f(w)|$. $D_w(f(x))=f(x)\oplus f(w+x)$

Theorem: $r_f(w)=2^{-n}\sum_u W_f(u)^2(-1)^{u\cdot w}$. For iterated ciphers, once the number of rounds is high enough to generate G (usually A_n), more rounds don't help.

AES: $8j+m$ component is $v_{(j,m)}$. $0=w_{0,(j,m)}+p_{(j,m)}+k_{0,(j,m)}$, $0=x_{i,(j,m)}w_{i,(j,m)}+1, i=1,2,\ldots,9$. $0=w_{i,(j,m)}+(Mx_{i-1})_{(j,m)}+k_{i,(j,m)}, i=1,2,\ldots,9$, $0=c_{(j,m)}+(M^*x_9)_{(j,m)}+k_{10,(j,m)}$. M is the combined effect of ShiftRow, MixColumn and the Linear diffusion. 5248 equations, 3840 sparse quadratic, 1408 linear diffusion, 7808 terms, 2560 state variables, 1408 key variables. $1280+1408=2588$ state/key variables eliminated, $4288-2688=1600$ unknown. 2688 equations, 1280 sparse quadratic, 5248 terms, 2560 state, 1408 linear diffusion, 1408 key variables.

For AES: $M: x\mapsto CRLx+63$ (Everything but subByte). Minimal polynomials: $C:(x^4+1)$, $R:(x^4+1)$, $L:(x+1)^3$, $C:(x+1)^{15}$. **BES:** $b\to M_Bb^{-1}+k_B$. $w_0=p+k_0$, $x_i=w_i^{-1}$, $w_i=M_Bx_{i-1}+k_i$, $c=M_B^*x_9+k_{10}$. $AES_k(P)=C\leftrightarrow BES_{\phi(k)}(\phi(P))=\phi(C)$, $\phi(a)=(a^{2^0},a^{2^1},a^{2^2},a^{2^3},a^{2^4},a^{2^5},a^{2^6},a^{2^7})$.

Circulant as linearized polynomial: $x\mapsto 0x05x^{2^0}+0x09x^{2^1}+0xf9x^{2^2}+0x25x^{2^3}+0xf4x^{2^4}+0x01x^{2^5}+0xb5x^{2^6}+0x8fx^{2^7}$, $S:w\mapsto\sum_{i=0}^{7}\lambda_iw^{255-2^i}+0x63$, modified: $S:w\mapsto\sum_{i=0}^{7}\lambda_iw^{-2^i}$. **Rank of system** is $\frac{equations}{monomials}$.

Equation Solving: If n =number of equations, M = number of variables. Solution takes 2^n, if $n=m$, n, if $n=m+1$ and $\sqrt{n}$ if $m>>n$.

Buchberger:
Input: $F=\{f_1,f_2,\ldots,f_m\}$. Output: Grobner $G=\{g_1,g_2,\ldots,g_s\}$.
$G\leftarrow F$;
Do {

$G' \leftarrow G$;
for$(p, q \in G', p \neq q)$ {
Compute $S(p, q)$;
$r \leftarrow REM(S(p, q), G')$;
if$(r \neq 0)$ {
$G' \leftarrow G' \cup \{r\}$;
}
}
} while$(G! = G')$

Theorem: Foregoing algorithm yields Grobner Basis.

F4/F5: Grobner by matrix reduction. *Example:* $f_1 = 3x^3yz - 5xy$, $f_2 = 5x^2z^2 + 3xy + 1$, $g_1 = xy - 2z$, $g_2 = x^2z - 3yz$.

	x^3yz	x^2z^2	yz^2	xy	z	1
f_1	3	0	0	-5	0	0
f_2	0	5	0	3	0	1
x^2zg_1	1	-2	0	0	0	0
$1g_1$	0	0	0	1	-2	0
zg_2	0	1	-3	0	0	0

Complexity of F5 is ${N_D}^\omega$ where N_D is the size of the largest matrix containing polynomials of degree D. If $m = n, D \approx .09n$.

Condition	Complexity
$m = an$	exponential in n
$n << m << n^2$	subexponential in n
$m = an^2$	polynomial in n

AES Design Criteria: Invertibility, minimize largest non-trivial correlation between input and output, minimize largest non-trivial xor, complexity of algebraic expressions, Simplicity of expression. Estimation of linearly independent equations for XSL on AES-128.

XL (extended linearization):
Input: $F = \{f_1, f_2, \ldots, f_m\}$.
Output: univariates.
$S \leftarrow \emptyset$;
Pick $D = d + 1$;
$G \leftarrow F$;
for$(i = 1; i \leq n + 1; i++)$ {
Generate $p_{\beta j} = x^\beta f_j, f_j \in F$;
Do Gaussian reduction.
If there is a univariate $f(x)$ {
Solve;
$S \leftarrow S \cup \{(x - a_i)\}$;
Substitute.
}
else

$D \leftarrow D + 1$;
}

For each round ($0 \le i \le 9$) and each S-box ($0 \le j \le 15$), we get $r = 8 \times 3 = 24$ quadratics. S: Total S-boxes, $P-1$: passive S-Boxes, Highest degree: $2P$. R: Equations. B: S-boxes/round. $|R| = \binom{S}{P}(t^P - (t-r)^P)$, $|R'| = \binom{S}{P-1}SB(N_r+1)(t-r)^{P-1}$, $|R''| = \binom{S}{P-1}(S_k - L_k)(N_r+1)(t-r)^{P-1}$, L_k: independent key variables, S_k: key variables. Total terms: $T = \binom{S}{P}t^P$. For $P = 2$, $(R + R' + R'') = 33,665,888, T = 33,788,100$. For $P = 3$, $(R + R' + R'') = 95.18 \times 10^9, T = 91.9 \times 10^9$.

Boomerang: $E = E_1E_0$. $E_0 : \alpha \to \beta, p$, $E_1^{-1} : \gamma \to \delta, q$. (1) Pick $P_1 \oplus P_2 = \alpha$; (2) Ask for $C_1 = E(P_1), C_2 = E(P_2)$; (3) Compute $C_3 = C_1 \oplus \gamma$, $C_4 = C_2 \oplus \gamma$; (4) Request $P_4 = E^{-1}(C_4)$, $P_3 = E^{-1}(C_3)$. $E_0(P_1) = I_1$, $E_0(P_2) = I_2$, $E_0(P_3) = I_3$, $E_0(P_4) = I_4$. $E_1^{-1}(I_1) = C_1$, $E_1^{-1}(I_2) = C_2$, $E_1^{-1}(I_3) = C_3$, $E_1^{-1}(I_4) = C_4$. What is probability that $P_3 \oplus P_4 = \alpha$? $e_1 : Pr[I_1 \oplus I_3 = \delta] = q$, $e_2 : Pr[I_2 \oplus I_4 = \delta] = q$. $Pr[e_1 \wedge e_2] = q^2$. $Pr[I_3 \oplus I_4 = \beta] = q^2$, $Pr[P_3 \oplus P_4 = \alpha] = p^2q^2$. If $(pq)^2 > 2^{-n}$, $pq > 2^{\frac{-n}{2}}$ and this is better than a simple differential attack if the differential probability is less than $2^{-n/2}$.

Amplified Boomerang: Use two short differentials instead of one differential. Start with quartet $P_1 \oplus P_2 = P_3 \oplus P_4 = \alpha$, each has $\alpha \to \beta$ with probability p. $E_0(P_1) \oplus E_0(P_2) = E_0(P_3) \oplus E_0(P_4) = \beta$. $E_0(P_1) \oplus E_0(P_3) = E_0(P_2) \oplus E_0(P_4) = \gamma$. $C_2 \oplus C_4 = C_1 \oplus C_3 = \delta$ and we want to use $\gamma \to \delta$. Probability that quartet becomes right is $\binom{Np}{2}2^{-n}q^2$. Distinguishers count quartets $((P_1, P_2), (P_3, P_4))$ satisfying $C_1 \oplus C_3 = C_2 \oplus C_4 = \delta$.

Bilinear Attack: Notation: $L_r[0, 1, 2, \ldots, n-1]$, $R_r[0, 1, 2, \ldots, n-1]$ are the input to round r and $I_r[0, 1, 2, \ldots, n-1]$, $O_r[0, 1, 2, \ldots, n-1]$ are the input (without key) and output to the round functions. If $\alpha \subseteq \{0, 1, 2, \ldots, n-1\}$, define $L_r[\alpha] = \bigoplus_{s \in \alpha} L_r[s]$. Consider the bilinear $L_{r+1}[\beta] \cdot R_{r+1}[\alpha] \oplus R_r[\beta] \cdot L_r[\alpha] = I_r[\beta] \cdot O_r[\alpha]$. TODO: More from Nick.

Square/Integral/Saturation Attack: Λ-set has 256 states which are either all the same in a byte position or all different. In either case $\bigoplus_{x \in \Lambda} x_{i,j} = 0$. *Structural:* Prior to MixCol $(x_0^i, x_1^i, x_2^i, x_3^i)^T$ and after $(y_0^i, y_1^i, y_2^i, y_3^i)^T$ then $y_0^0 \oplus y_1^0 \oplus \ldots \oplus y_{255}^0 = 00$. guess key byte. If condition holds, it's right; otherwise it isn't. Mixcolumn is the only operation that changes this condition and only if there is more than one active byte in the column. To capitalize on this at final round (where mixing disrupts condition), Gives one linear combination of 4 key bits in round 4. Properties of sets of texts preserved by encryption. *Example:* 256 plaintexts that agree on 15 input bytes. θ - linear map, γ - non-linear transform, π - byte transposition, σ - key addition, Λ - 256 active states, λ - set of indices of active bytes. Then $\bigoplus_{b=\theta(a), a \in \Lambda} b_{i,j} = 0$. $\forall x, y \in \Lambda$, $x_{i,j} \neq b_{i,j}$ if $(i,j) \in \lambda$, $x_{i,j} = b_{i,j}$ if $(i,j) \notin \lambda$. $a_{i,j} = b_{i,j} \oplus S_\lambda[b_{i,j}] \oplus_{i,j} k_{i,j}^4$; if the result is not balanced (over Λ), the key is wrong. *Example with block cipher Square:* Square round is $\rho_r(x) = \sigma_r(\pi(\gamma(\theta(x))))$, γ is the non-linear substitution, θ is linear diffusion (c_i are polynomials), π flips rows and columns, σ_r is key addition. $\bigoplus_{b=\theta(a), a \in \Lambda} b_{i,j} = \bigoplus_{a \in \Lambda} \bigoplus_k c_{j-k} a_{i,k} = \bigoplus_l c_l(\bigoplus_{a \in \Lambda} a_{i,l+j})$. After three rounds, all bytes are active. For ciphertext $d_{i,j}$, guess $k_{i,j}^4$ and compute $b_{j,i} = \gamma^{-1}(d_{i,j} \oplus k_{i,j}^4)$.

Truncated differentials: Suppose $g : GF(2)^n \times GF(2)^n \times GF(2)^m \to GF(2)^n \times GF(2)^n \times$ implements a Feistel cipher round that is $g(X, Y, Z) = (Y, f(Y, Z) \oplus X)$. The S/N ratio is $\frac{|K|p}{\gamma\lambda}$ where p is the differential probability, γ is the number of suggested keys and λ is the ratio of non-discarded keys to all keys. A full differential $a' \to b'$ specifies all n bits, a truncated differential specifies a subset of bits. Here is an example of its usefulness. Let $f(x) = x^{-1}$. It has non-linear order $n-1$. If n is odd the map is differentially 2-uniform $p = 2^{1-n}$; if n is even the map is differentially 4-uniform $p = 2^{2-n}$. For 3 rounds, the differential probability is 2^{3-2n} and the S/N is 2^{3-n}. For $r > 3$ the attack can't succeed. For 2 rounds, $p = 2^{1-n}$ and the S/N is 2^{n+1} so the attack requires 2^n texts and is $O(2^{3n})$ but for $a' \neq 0$, there are only 2^{n-1} possible b' and we get

one bit of information — the S/N is $\frac{2^{2n}}{2^{2n-1}} = 2$. Let $f(x,k)$ be the non-linear function in a 5 round Feistel cipher with block size $2n$. Let $\alpha \neq 0$ be an input differential for which only a fraction, W, of all output differences are possible. Then a truncated differential attack requires $2L$ chosen plain-cipher pairs and is $O(L2^{2n})$ where L is the smallest integer: $W^L < 2^{-2n}$. Note that truncated differentials cannot propagate backwards.

Higher order differentials: Define

$$\Delta_a^{(1)}(f(x)) = f(x+a) - f(x), \Delta_{a_1,a_2,\ldots,a_i}^{(i)}(f(x)) = \Delta_{a_i}^{(1)}(\Delta_{a_1,a_2,\ldots,a_{i-1}}^{(i-1)}(f(x))).$$

Let $L[a_1,a_2,\ldots,a_i]$ is the set of all linear combinations of $\langle a_1,a_2,\ldots,a_i\rangle$. Then $\Delta_{a_1,a_2,\ldots,a_i}^{(i)}(f(x)) = \sum_{\gamma\in L[a_1,a_2,\ldots,a_i]} f(P+\gamma)$ and $ord(\Delta_a^{(1)}(f(x))) \leq ord(f(x)) - 1$. Here is an example application. Let $f(x,k) = (x+k)^2 \pmod p$ be the Feistel round function with size is $lg(p)$. f is differentially 1-uniform and the round differential has probability $\frac{1}{p}$, $f''(x)$ is constant. The first order differential attack on a 5 round cipher requires $2p$ texts and is $O(p^3)$; a second order differential attack requires 8 texts and is $O(p^2)$. [Use $\Delta_{\alpha,\beta}(f(x)), \alpha = a||0, b = b||0, S/N = r^2$]. For a 5 round Feistel with f non-linear of degree r using an rth order differential requires 2^{r+1} texts and is $O(2^{2n+r})$.

SFLASH attack: The idea of SFLASH is to hide an easy-to-invert quadratic map, $F(x)$ with two "secret" invertible linear transformations U,T. If $e = q^i + q^j$, $F(x) = x^e$ is quadratic; in particular, if $e = q^\theta + 1$ (and from now on, it is) and $P = T \circ F \circ U$, F is (easily) invertible if $(q^\theta+1, q^n-1) = 1$ (so $q = 2^k$) but without knowledge of U,T, P isn't. This is the C^* scheme Patarin broke. If we remove r of n quadratic equations in the base field that represent P, Patarin's attack doesn't work and the new scheme C^{*-} can be used for signatures. Let $\Pi : (x_1,x_2,\ldots,x_n) \mapsto (x_1,x_2,\ldots,x_{n-r})$. P is public key; to sign m, choose r coordinates at random. Signer recovers s: $P_\Pi(s) = \vec{r}$. Signature is (m,s). The idea of Shamir's attack is to use a multiplicative property of the linear transformation induced by a field element, ξ, on the differential to obtain a different set of linear combinations of the F quadratics and then apply Patarin's attack. Define the differential $DF(a,x) = F(x+a) - F(x) - F(a) - F(0)$. For $F(x) = x^e$, $e = q^\theta + 1$ in field of characteristic q, $DF(\xi\cdot a, x) + DF(a, \xi\cdot x) = (\xi + \xi^{q^\theta})DF(a,x)$. Denote M_ξ as the matrix for the linear transformation induced by multiplying by ξ, $L(\xi)$ as the matrix induced by $\xi + \xi^{q^\theta}$ and $\Lambda(L(\xi)) = T_\Pi M_{L(\xi)} T^{-1}$. Let Q be the space of quadratic forms, V the subspace generated by TFU and V_Π the space generated by $T_\Pi FU$. $V_\Pi \subseteq V \subseteq Q$. There is a corresponding set of bilinear forms B, and sets W and W_Π and setting $N_\xi = U^{-1}M_\xi U$, the relation $DP(N_\xi(a),x)) + DP(N_{a,\xi}(x)) = \Lambda(L(\xi))DP(a,x)$ holds. This equation relates unknown coefficients of N_ξ on the left with unknown coefficients of $\Lambda(L(\xi))$ on the right. Setting $S_M(a,x) = DP_\Pi(N_\xi(a),x)) + DP_\Pi(N_{a,\xi}(x))$ we note the LHS is in W_Π with probability q^{-r} if M represents a matrix for some ξ induced value and probability $q^{n^2/2}$ if not. These identify transforms that can produce other P equations to fill out the r unknown quadratics to apply Patarin. SFLASH-1 parameters: $q = 2^7, n = 37, \theta = 11, r = 11$; SFLASH-2 parameters: $q = 2^7, n = 67, \theta = 33, r = 11$.

Impossible differentials: Suppose $\alpha \to \beta$ for E_1 is impossible and $E = E_2 \circ E_1 \circ E_0$. Encrypt many plaintexts with possible output α after E_0 and decrypt pairs with all possible subkeys through E_2. If these suggest $\alpha \to \beta$ the keys are impossible.

Related Key Attacks: If $K \to (K_1,K_2,\ldots,K_r)$ and $K^* \to (K_2,\ldots,K_r,K_1)$ and $F(X,K_i)$ is the round function then $n-1$ of the rounds are identical. If $P^* = F(P,K_1)$ and we know $2^{n/2}$ P/C pairs $(P,C)_K$ and $2^{n/2}$ P/C pairs $(P^*,C^*)_{K^*}$ try to solve $F(P,K') = P^*$ and $F(C,K') = C^*$; this gives K_1. Related key differential: $\alpha \to \beta$ for E^0 with $p > 2^{-n}$ then $Pr_{X,K}[E_K^0(X) \oplus E_{K\oplus\Delta K}^0(X\oplus\alpha) = \beta] = p > 2^{-n}$.

Slide Attack: Let F be a per-round function. If $C = E_K(P) = F_K^m(P), P, C \in GF(2)^n$ and $P' = F(P)$ then $C' = E(P') = F(C)$. To find slide pairs, let $\alpha_F(P, C) = K$ which is easy to calculate. Store $2^{n/2}$ (and possibly less as in DES) pairs (P, C) if $\alpha_F(P, C) = \alpha_F(P', C')$, $P' = F_K(P)$ and $C' = F(C)$. By birthday collision, this will happen. Effective against rounds which implement weak permutations.

Wiedemann: Solve $A\vec{x} = \vec{b}$ in $O(n\omega)$ time over $F = GF(q)$ where ω is the number of non-zero elements of A. Let $S = \langle A^i b \rangle, det(A) \neq 0$ and suppose $f(z) = \sum_{j=0}^{d}$ is the minimal polynomial normalized so the trailing coefficient (f_0) is 1. Let $x = -\sum_{i=1}^{d} f_i A^{i-1} b$. Then $Ax = (1 - f(A))b = b$ so x is a solution, this requires $2n(\omega + 1)$ field operations. To find f, look at the *linear recurrent sequence* $s_i = (u, A^i b)$, the associated polynomial $f_u | f$ can be computed from the first $2n$ terms is $O(n^2)$.

Let $F = GF(q)$. Every kth order linear recurrent sequence is ultimately periodic with period r satisfying $r \leq q^k$ ($r \leq q^k - 1$ if homogeneous). If $s_{n+k} = a_{k-1}s_{n+k-1} + \ldots + a_0 s_n$ the associated matrix is $A = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & 0 & a_0 \\ 1 & 0 & 0 & \ldots & 0 & 0 & a_1 \\ 0 & 1 & 0 & \ldots & 0 & 0 & a_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & 1 & a_{n-1} \end{pmatrix}$ and the least period divides $A^k - 1$. If $D_n^{(r)} = \begin{pmatrix} s_n & s_{n+1} & s_{n+2} & \ldots & s_{n+r-1} \\ s_{n+1} & s_{n+2} & s_{n+3} & \ldots & s_{n+r-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ s_{n+r-1} & s_{n+r} & s_{n+r+1} & \ldots & s_{n+2r-1} \end{pmatrix}$ then $s_0, s_1, \ldots$ is a linear recurrent sequence iff $D_n^{(r)} = 0$ for all but finitely many $n \geq 0$. If a linear recurrent sequence has minimal polynomial $m(x)$ of degree $\leq k$ and $r = \lfloor k + \frac{1}{2} - \frac{1}{2} m_{2k} \rfloor$ then $m(x) = x^r g_{2k}(\frac{1}{x})$ and $m(x)$ depends only on the first $2k$ terms.

```
Wiedemann's Algorithm
1. Set b[0]= b, k=0, y[0]= 0, d[0]= 0
2. If b[k]=0, x= -y[k].  Terminate.
3. Select u[k+1] at random
4. Compute first 2(n-d[k]) terms of (u[k+1], A**i b[k])= s[0,..]
5. Set f[k+1](z)= minimum poly in 4
6. Set y[k+1]= y[k]+f[k+1](z) b[k], b[k+1]= b[0]+A[y[k+1]), d[k+1]= d[k]+deg(f[k])
7. k= k+1, go to 2

Berlekamp's Algorithm
Given s[0], s[1], ... with generating function G(x)= s[0] + s[1]x + ... + s[i] x**i + ... in
F=GF(q)

1. g[0](x) = 1, h[0](x)=x, m[0]= 0
2. b[j]= coefficient of x**j in G(x) g[j](x)
   g[j+1]= g[j](x)- b[j] g[j](x),
   h[j+1] = 1/b[j] x g[j(x), if b[j] !=0 and m[j] >=0; x h[j](x), otherwise
   m[j+1]= -m[j], if b[j] !=0 and m[j] >=0; m[j+1]+1, otherwise

Version 2
Input: F=GF(q), 2n coefficients of a Linear recurrence <a[0], a[1], ..., a[2n-1]>
Output:  Minimal polynomial P
```

j	$g_j(x)$	$h_j(x)$	m_j	b_j
0	1	x	0	0
1	1	x^2	1	2
2	$1+x^2$	$2x$	-1	1
3	$1+x+x^2$	$2x^2$	0	0
4	$1+x+x^2$	$2x^3$	1	2
5	$1+x+x^2+2x^3$	$2x+2x^2+2x^3$	-1	2
6	$1+x^3$	$2x^2+2x^3+2x^4$	0	1
7	$1+x^2+2x^3+x^4$	$x+x^4$	0	1
8	$1+2x+x^2+2x^3$	-	0	-

Figure 3.1: Berlekamp-Massey for $G(x) = 1 + x + x^4 + x^6 + x^7 \in F_2[x]$

```
R0=x**(2n); R1= a[0]+a[1]x+ ... + a[2n-1] x**(2n-1); V0=0; V1=1;
while(n<=deg(R1) {
     R0= QR1+R;  // Division Algorithm
     V= V0-Q V1;
     V0= V1; V1= V; R0= R1; R1= R;
     }
d= max(deg(V1), 1+deg(R1));
P= x**d V1(1/x);
return(P/leading-coeff(P));
```

3.11 Quantum Crypto

Key Distribution: Choose two basis: $B_1 = (|0\rangle, |1\rangle)$ and $B_2 = (|\frac{1}{2}\rangle, |-\frac{1}{2}\rangle)$. Alice chooses a random sequence of basis β_i from $\{B_1, B_2\}$ and a random sequence of bits b_i and encodes $b_i with \beta_i$. Bob chooses a random sequence of basis β_i from $\{B_1, B_2\}$ and obtains sequence $c_i = \beta_i b_i$. Bob reveals his sequence of basis choices and then Alice reveals hers. Each confirms subset of bits for which the sequences agree using some classical system.

Consider three polarizers A, B, C which have phases $0, 45, 90$. If A and C are placed in series, no light comes through but if A, B and C are placed in series, some light gets through. Let $|0\rangle, |1\rangle$ be two orthogonal vectors in a complex $2-$dimensional space. A *qubit* is a unit vector in this space. It can have many basis. *Shor:* Choose $m : n^2 \leq 2^m < 2n^2$ and let $v = \frac{1}{\sqrt{2^m}}(|0\rangle + |1\rangle + \ldots + |2^m - 1\rangle$. Let f be a function and $x = \frac{1}{C}\sum |x\rangle$. System computes $t = \frac{1}{C}\sum |x, f(x)\rangle$. If $f(x) = a^x \pmod n$, measurement of last $\frac{m}{2}$ bits fixes sequence $t = \frac{1}{C}\sum |x, u = f(x)\rangle$ for fixed u measuring the Fourier transform identifies period, that is $m : a^i = a^{i+r}$ so that $a^r = 1 \pmod n$ but that means r is a universal exponent and we can (probably) factor n.

Universal exponent method: Suppose $a^r = 1 \pmod n, \forall a : (a, n) = 1$. Put $r = 2^k m$, m odd. Choose a at random if $(a, n) \neq 1$, we have a factor; otherwise, put $b_0 = a^m \pmod n$ and $b_{n+1} = b_n^2 \pmod n$. If $b_0 = 1$ or $b_j = -1 \pmod n, 0 \leq j < k$ or $b_{j+1} = 1 \pmod n$ and $b_j = -1 \pmod n$, stop and pick a new a. If $b_{j+1} = 1 \pmod n$ but $b_j \neq \pm 1 \pmod n$ then $(b_j - 1, n)$ is a factor.

3.12 Protocols, Models

Bell-Lapadula (BLP): Subjects and Objects labeled. Simple Security property: S can read O iff $L(O) \leq L(S)$. *-Property: S can write O iff $L(S) \geq L(O)$. *Tranquility:* Labels never change. *Biba:* S can write O iff $I(O) \leq I(S)$. S can read O iff $I(S) \leq I(O)$.

Perfect Forward Security and ephemeral Diffie-Hellman with authentication: Both Alice and Bob agree on modulus p and base g. Alice picks secret a and Bob b for signing; signing public keys have been previously exchanged. So for the session key, Alice picks random x and Bob picks random y. In the protocol below, $r_A = g^x \pmod p$, $r_B = g^y \pmod p$ and $K = g^{xy} \pmod p$. (1) $A \to B$: "Alice", r_A. (2) $B \to A$: "Bob", r_B, $E_K(sig_B(r_A, r_B))$ (3) $A \to B : E_K(sig_A(r_A, r_B))$. Throwing away r_A, r_B, x, y yields perfect forward secrecy.

Kerberos (v4): L is lifetime. T_X is the timestamp from X. Most features (like lifetime) prompted by workstation/server model (no longer valid), network masquarading replay. Kerberos AS is sole root of trust for realm.

1. $A \to S$: A, B
2. $S \to A$: $\{T_S, L, K_{AB}, B, \{T_A, L, K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$.
3. $A \to B$: $\{T_S, L, K_{AB}, A\}_{K_{BS}}, \{A, T_A\}_{K_{AB}}$.
4. $B \to A$: $\{T_A + 1\}$.

Protocol layers: Application (DNS, TLS, HTTP, SSH), Transport (TCP), Network (IPv4), Link (ethernet, Wi-Fi).

X.509 certificate format: Version number (There are three), CA serial number, Signature algorithm (useless, appears later), Issuer name (x.509 name), validity period, subject name (x.509), subject public key information, Issuer unique identifier (x.509, optional), subject unique id (x.509, optional), extensions (version 3), signature. Extenstions required because (1) Subject/issuer identifiers inadequate, (2) no way to tie policy to cert, (3) cannot constrain use, (4) cannot easily cross reference entities for better key management. Extensions include: Authority key ID, Subject key ID, Key usage, Private key validity period, certificate evaluation policies, policy map between CAs, alternate subject and issuer names, basic, name and policy constraints.

TLS: Three phases: (1) Peer negotiation, (2) PK based key exchange (including certificate exchange), (3) encrypted traffic. TLS exchanges records each record has a content-type and MAC; all records are numbered. Content type 22 is handshake. Results in 2 encryption keys, 2 integrity keys and 2 IV's.

M1: ($C \to S$) ClientHello(Client-random[28], cipher-suites, compression methods, highest protocol version),

M2: ($S \to C$) ServerHello(ServerRandom[28], cipher-suite, certificates),

M3: ($C \to S$) ClientKeyExchange(E(PkS, Pre-Master Secret), MD5-SHA1(M1 —— M2—— M3A)), [Master Secret is PRF(Pre-master secret, "master secret", ClientRandom —— ServerRandom)],

M4: ($S \to C$) Finish MD5-SHA1(M1 —— M2 —— M3A —— M3C).

IPSEC: Two protocols: securing packets and key negotiation. Two modes: transport and tunnel. In transport mode only payload is encrypted. Packets can be secured for authentication and integrity only

(AH) or authentication, confidentiality and integrity. IKE Phase1: CP (crypto proposed), CS (crypto selected), IC (initiation cookie), RL (response cookie), $K = h(IC, RC, g^{ab} \pmod p), R_A, R_B)$. $SKEYID = h(R_A, R_B, g^{ab} \pmod p))$. $Proof_A : [h(SKEYID, g^a \pmod p), g^b \pmod p), IC, RC, CP, \text{“}Alice'']_{Alice}$. Public Key: (1) $A \rightarrow B$: IC, CP. (2) $B \rightarrow A$: IC, RC, CS. (3) $A \rightarrow B$: IC, CP $g^a \pmod p), \{R_A\}_{Bob}, \{\text{“}Alice''\}_{Bob}$. (4) $B \rightarrow A$: IC, CP $g^b \pmod p), \{R_B\}_{Alice}, \{\text{“}Bob''\}_{Alice}$. (5) $A \rightarrow B$: IC, CP $E(Proof_A; K)$. (6) $B \rightarrow A$: IC, CP $E(Proof_B; K)$.

Fiat-Shamir: Prove knowledge of a secret, s, where $v = s^2 \pmod n$, $n = pq$; v, n, public. A proves she knows s: (1) A picks r at random and computes $x = r^2 \pmod n$ — commitment, (2) B chooses $e \in \{0, 1\}$ at random and sends e to A — challenge, (3) A computes $y = rs^e \pmod n$ and sends it to Bob — response, (4) finally, B verifies $y^2 = r^2 s^{2e} = xv^e \pmod n$ — verify this.

S/Mime:

```
DSig:
<Signature>
  <SignedInfo>
    <CanonicalizationMethod/>
    <Reference URI=?>
      <Transforms/>
      <DigestMethod/>
      <DigestValue/>
  </SignedInfo>
  <SignatureValue/>
  <KeyInfo/>
  <Object>
</Signature>

XML Encryption:
<EncryptedData>
  <EncryptionMethod/>
  <KeyInfo>
    <AgreementMethod/>
    <KeyName/>
    <RetrievalMethod/>
  </KeyInfo>
  <CipherData/>
</EncryptedData>

SAML: Authn/AuthZ Request/Response over SOAP.
      Assertion, conditions, advice.
XACML: Authorization Rules:
      Subjects, Resources, Actions.
REL: Grant, Principal, Right, Resource, Condition.
WS-Policy: security policy
WS Trust: Trust
WS-Privacy including WS-Secure
   Conversation, Federation.
WS-Authorization: Principal, Claim, Token.
```

More Timings: P4, 2.1 GHz. AES: 44 operations/round.

Algorithm	Key Size	Speed(MB/sec)	Algorithm	Key Size	Speed(MB/sec)
DES	56	21	3DES	168	9.8
SHA-1	NA	68	SHA-256	NA	44
TEA	64	23	AES	128	61

Reestimation: Rotor modeled by $S(r_j, R) = C^r RC^{-r}$ and represented by a $q \times q$ permutation matrix. Key space is $D_1 \times D_2 \times \ldots \times D_k$, D_i is all $q!$ permutation matrices. ${\chi^{cs}} = {\chi_1}^{cs} \times {\chi_2}^{cs} \times \ldots \times {\chi_k}^{cs}$, ${\chi_i}^{cs}$ is all possible $q \times q$ stochastic matrices. Suppose $\vec{p}$ is plaintext distribution. $d(r, x) = S(r, x)\vec{p}$. Likelihood $L(X|\{c, r\}) = Pr(ciphertext = \{c_1\}^N|\{r_1\}^N; X) = \prod_{n=1}^{N} {e_{c(n)}}' d(r(n); X)$. Want to maximize L by adjusting X. The MLE of X exists and is strongly consistent. Use the following result: Let $P(z)$ be a polynomial with non-negative coefficients homogeneous of degree d in z_{ij}, $\mathcal{Z} = \{z_{ij} : z_{ij} \geq 0, \sum_i^{q_j} z_{ij} = 1\}$. $\mathcal{T}(z)_{ij} = z_{ij} \frac{\frac{\partial P}{\partial z_{ij}}}{\sum_i^{q_j} z_{ij} (\frac{\partial P}{\partial z_{ij}})_z}$. Computations requires is $\approx kq^2N$ and a 2 rotor machine with $N = 1024$ ciphertext letters requires about 60 iterations.

3.13 Random Number Quality

Motivation: Traditional approach for getting n bit value: (1) Get large sample. (2) Calculate the relative frequency, r_w, of each word w in b-bit block. (3) Estimate $H = -\sum_{w=0}^{2^r-1} r_w lg(r_w)$. Repeat $\frac{n}{H}$ times. Total bits checked: $\lceil \frac{nb}{H} \rceil$ Concern: small set of possible values and deterministic mixing reduces entropy. Entropy is not the best measure of security. Consider the following:

Theorem. The entropy of a source $P = \langle < p_1, p_2, \ldots, p_N \rangle$ which is mixed by $F : [1..N] \rightarrow [1..m]$ is greater than the entropy of the mixed sequence.

Proof: Let $Prob(O = j) = q_j$ and $Q = \langle q_1, q_2, \ldots, q_m \rangle$. $H_{out} = H_Q = -\sum_{j=1}^{m} q_j lg(q_j) = -\sum_{j=1}^{m} [\sum_{f(i)=j} p_i] lg([\sum_{f(i)=j} p_i]) = -\sum_{i=1}^{N} p_i lg(p_i + S_i) < H_p = H_{in}$, where $S_i = \sum_{j \neq i, F(i)=F(j)} p_j$ for the standard Shannon entropy $H_Q = -\sum_{i=1}^{N} p_i lg(p_i)$.

Observation: Suppose T values are required in cryptoperiod; if $Q = \langle q_1, q_2, \ldots, q_m \rangle$ is the distribution and $q_{i_1} \geq q_{i_2} \geq \ldots \geq q_{i_m}$, adversary's best strategy is to guess $\langle i_1, i_2, \ldots \rangle$ until success. This motivates a different entropy measure. Define $H_\alpha(Q) = \frac{1}{1-\alpha} \sum_{j=1}^{M} {q_j}^2$. $H_2(Q)$ is a good measure for collision resistance (not secrecy) since $\sum_{j=1}^{m} {q_j}^2 = 2^{-H_2(Q)}$; the waiting time for repeats is $\sqrt{\pi 2^{H_2(Q)-1}}$. $H_\infty(Q)$ is a good measure for the quality of resulting key generation, since the expected cost of the guessing attack is $\frac{1}{2q_{max}} = 2^{H_\infty(Q)-1}$. As an example, consider the distribution, Q over 128 bit quantities consisting of one value that occurs with probability 2^{-80} and is otherwise flat. $H_2(Q) \approx 128$, $H_\infty(Q) \approx 80$.

Definition: If X is a event with n possible outcomes having respective probabilities $p_1, p_2, \ldots, p_n$ the *min-entropy* of X is $H_\infty(X) = min_{1 \leq i \leq n} - lg(p_i) = -lg(max_i(p_i))$. To get an estimate of the min-entropy or $W(Q)$, we need $S(Q)$. Suppose randomizer produces $m = 2^n$ outputs with probability distribution $Q = \langle q_1, q_2, \ldots, q_m \rangle$. Quality of Q is $S(Q) = \sum_{j=1}^{m} q_j^2 \geq \frac{1}{m}$ which is the probability of repeated output. $W(Q) = \sum_{j=1}^{m} j q_j \leq \frac{m+1}{2}$ which is the adversary's work factor. Estimating either $H_2(Q)$ or $H_\infty(Q)$ consists of four steps. (1) Form Markov model of input source data (over L consecutive samples), (2) Compute source data repeat probability, (3) Estimate $S(Q)$, (4) Use $S(Q)$ to estimate lower bound on $W(Q)$ and/or $H_\infty(Q)$.

Entropy Order Paradox: Consider $Q_1 = \langle 0.258, 0.116, 0.146, 0.032, 0.140, 0.266, 0.038, 0.004 \rangle$ and $Q_2 = \langle 0.256, 0.232, 0.076, 0.130, 0.006, 0.157, 0.005, 0.129 \rangle$. $H(Q_1) = 2.54542$ and $H(Q_2) = 2.54495$ but $S(Q_1) = 0.194176$ and $S(Q_2) = 0.188076$ while $W(Q_1) = 2.844$ and $W(Q_2) = 2.903$.

Step 1 - Markov Model: The model consists of $\Theta = \langle \theta_1, \theta_2, \ldots, \theta_L \rangle$ states where where ρ is the initial probability distribution, and $T = \begin{pmatrix} \tau_{1,1} & \tau_{1,2} & \ldots & \tau_{1,s} \\ \tau_{2,1} & \tau_{2,2} & \ldots & \tau_{2,s} \\ \ldots & \ldots & \ldots & \ldots \\ \tau_{s,1} & \tau_{s,2} & \ldots & \tau_{s,s} \end{pmatrix}$ is the transition matrix. The procedure is to (1) Model source as sequence of states $\langle s_1, s_2, \ldots, s_s \rangle$, (2) Get ρ (use steady state estimate), (3) Determine state defining bits. For multiple sources, $\Theta^{(k)} = \langle \theta_1, \theta_2, \ldots, \theta_{i_k} \rangle$ and $\sum_{i=1}^{N} {p_i}^2 = \sum_{i_1=1}^{N_1} (p_{i_1}^{(1)} p_{i_2}^{(2)} \ldots p_{i_k}^{(k)})^2$. **Step 2 - Compute source data repeat probability:** $\sum_{j=1}^{N} {p_j}^2 = [\rho_1, \rho_2, \ldots \rho_s] T [1, 1, \ldots, 1]^T$. **Step 3 - Estimate $S(Q)$:** $S(Q) = \sum_{j=1}^{m} q_j^2 = \frac{1}{m}(1 + \epsilon_s)$ where $(1 + \epsilon_s) = (m-1) \sum_{i=1}^{N} p_i^2$. **Step 4 (for H_2) - Estimate $W(Q)$ using $S(Q)$ for L source inputs:** To get the best possible bound on $W(Q)$ given $S(Q)$ (q_j unknown): Let $m' = min(m, \frac{3S(Q)+4+\sqrt{9S(Q)^2+16}}{6S(Q)}) \approx min(m, \frac{4}{3S(Q)})$ then $W(Q) \geq B$ where $B = \frac{1}{6}(3m' + 3 - \sqrt{3(m'^2-1)(m'S(Q)-1)})$. To obtain this result use Lagrange multipliers to

minimize $W(Q)$ subject to $\sum_{j=1}^{m} {q_j}^2 = S(Q)$ and $\sum_{j=1}^{m} q_j = 1$. **Step 4 (for H_∞):** Use Dynamic Programming compute p_{max} or proceed as follows: Set $y_1 = F(x_1)$, $q_1 = Pr[y_1] = p_{max} + \sum_{i=2}^{N} p_i I_{i,1}$ and $q_j = \sum_{i=2}^{N} p_i I_{i,j}$. $\mu_1 = E[q_1] = \frac{1}{M}[1 + (M-1)p_{max}]$, $\mu_2 = E[q_j] = \frac{1}{M}[1 - p_{max}]$, $\sigma_1^2 = \sum_{i=2}^{N} p_i{}^2 Var(I_{i,1}) = (\frac{1}{M} - \frac{1}{M^2}) \sum_{i=2}^{N} p_i{}^2$ and for $j \geq 2$, $\sigma_j^2 = \frac{M-1}{M} \sum_{i=2}^{N} p_i{}^2$. $-lg(\mu_1)$ is a good estimate for $H_\infty(Q)$. Want $|-lg(\mu_1) - H_\infty(Q)| \leq \frac{1}{2} 10^{s-d+1}$, whereas s is largest integer: $10^s \leq H_\infty(Q)$. If Y is the number of q_j exceeding B, $Pr[q_{max} \leq B] = 1 - Pr[Y > 0] \geq 1 - E[Y] > 1 - \epsilon$. $Pr[E_j] = Pr[z > \frac{\mu_1^{1-\frac{1}{2}10^{-d}}}{\sigma}, j > 1$. Put $B = max(\mu_1 + T_1\sigma, \mu_2 + T_2\sigma)$, where z is normally distributed and $Pr(z > T_1) = \frac{\epsilon}{3}$ while $Pr(z > T_2) = \frac{\epsilon}{3(M-1)}$ then $Pr(\mu_1^{1+\frac{1}{2}10^{-d}} \leq p_{max} \leq \mu_1^{1-\frac{1}{2}10^{-d}}) \geq (1 - \epsilon)$.

Example ($L = 3$): Let b_t, b_{t+1}, b_{t+2} be three successive states and $Prob(b_{t+2} = b_{t+1} \oplus b_t) = .8$ with $s = 4$ states then $T = \begin{pmatrix} .8 & .2 & 0 & 0 \\ 0 & 0 & .2 & .8 \\ .2 & .8 & 0 & 0 \\ 0 & 0 & .8 & .2 \end{pmatrix}$ and the initial distribution $\rho = (.25, .25, .25, .25)$. The state distribution is $\Theta = \langle \theta_1, \theta_2, \theta_3 \rangle$. In SHA-1 mixing example, $\sum_{i=1}^{N} p_i^2 = 4.87 \times 10^{-44}$, $L = 256$ and we compute $S(Q) = \sum_{i=1}^{m} q_j^2 \approx \frac{1}{m}[1 + (m-1)\sum_{i=1}^{N} p_i^2]$. $m = 2^{160}$. $m = 2^{160}$, $m' = 2.74 \times 10^{43}$, $W(Q) \geq 9.1 \times 10^{42}$.

Parameter Estimate: $N = \alpha \Gamma^{L-1} U$, α is initial ρ, Γ is initial T. $U = [1, 1, \ldots, 1]^T$. $I_{i,j}$ is 1 if $F(i) = j$ and 0 if $F(i) \neq j$. $q_j = \sum_{i=1}^{N} I_{i,j} p_i$, $E(q_j) = \sum_{i=1}^{N} p_i E(I_{i,j}) = \frac{1}{m}$. $Var(q_j) = \sum_{i=1}^{N} p_i^2 Var(I_{i,j})$. $Var(I_{i,j}) = \frac{1}{m} - \frac{1}{m^2}$. $Var(q_j) = \sum_{i=1}^{N} p_i^2 Var(I_{i,j}) = \frac{m-1}{m^2} \sum p_i^2$. $E(\sum_{j=1}^{m}) q_j^2) = \sum_{i=1}^{N} E(q_j^2) = \sum_{j=1}^{N} E(q_j^2) + Var(q_j) = \frac{1}{m}(1 + (m-1)\sum_{i=1}^{N} p_i^2$.

Extension to HMM: Transition matrix $T = \tau_{i,j}$, s states, $\vec{\rho}$ initial distribution, $\theta_t \in \{1, 2, \ldots, r\}$ is the output at time t, $C^{(n)} = (c_{i,j}^{(n)})$, $c_{i,j}^{(n)} = \sum_{\theta_1, \ldots, \theta_n} Pr(\theta_1, \ldots, \theta_n, \sigma_n = i) Pr(\theta_1, \ldots, \theta_n, \sigma_n = j)$. $\sum_{i,j} c_{i,j}^{(n)} = \sum_{i=1}^{N} p_i^2 = \sum_{\theta_1, \ldots, \theta_n} Pr(\theta_1, \ldots, \theta_n)^2$ and $C^{(n)} = (BB^T) \cdot (T^T C^{(n-1)} T)$ where $\cdot$ means elementwise multiplication. Recursion step requires $2s^3$ multiplications. ≈ 7 minuses for 400 outputs without eigenvalue.

Definitions: $f : G \to \mathbb{C}$, $g : G \to \mathbb{C}$, $E(f) = E(g) = 0$, $E(|f|^2) = E(|g|^2) == 1$. $S_{fg} = f(x) \cdot \overline{g(y)}$, $L_{ab}(X, Y) = \chi^a(x)\chi^{-b}(y)$. Imbalance of S: $I(S) = |E(S)|^2$, $\overline{I}(S) = \frac{1}{K} \sum_{k \in K} I(S|K = k)$. $C = (c_{ab}), c_{ab} = \overline{I}(L_{ab}(X, Y))$, $a, b \in G \backslash \{0\}$. Let $y = e_k(x) = x + k$, $c_{ab} = \delta(a \oplus b)$. $c_{ab} = \frac{1}{|K|} \sum_k |\mathcal{F}(\chi^b \cdot e_k)(a)|^2$, $\overline{I}(S) = \hat{f}^T C \hat{g}$. $\hat{f}_a = |\mathcal{F}(f)(a)|^2$, $\hat{g}_b = |\mathcal{F}(g)(b)|^2$. The *likelihood estimate of correlation* is $\tilde{I}(S) = |\frac{1}{N} \sum_{x,y} f(x)\overline{g(\tilde{y})}|^2$. $\xi(x, J, N)$ is the *imbalance distribution* with imbalance parameter J. $\xi(x, J, N) \frac{2N}{1-J} h(\frac{2N}{1-J} x, \frac{2N}{1-J} J)$ where $h(\cdot, s)$ is the probability density of χ^2 with 2 degrees of freedom and skewness parameter s. $\xi(x, J, N) = \frac{N}{(1-J)\sqrt{\pi}} e^{-\frac{N(x+J)}{1-J}} \sum_{r=0}^{\infty} \sigma_r$ where $\sigma_r = \frac{1}{(2r)!}((\frac{2N}{1-J})^2 Jx)^r \frac{\Gamma(r+\frac{1}{2})}{\Gamma(r+1)}$. If $J << (\frac{1}{2N})^2$, $\xi(x, J, N) \approx h(x, J, N)$, $h(x, J, N) = \frac{N}{1-J} e^{-\frac{N(x+J)}{-1J}}$ with accumulated error $\epsilon = 1 - e^{-\frac{JN}{1-J}}$.

Let S be an I/O product and $S_1, \ldots, S_N$ samples, $\tilde{I}(S) = |\frac{1}{N} \sum_{j=1}^{N} S_j|^2$. Let E be an $n-1 \times n-1$ matrix with $E_{ij} = \frac{1}{n-1}$ and C the truncated correlation matrix. $C^r - E = (C - E)^r$ and $\sigma_2(C) = \sigma_1(C - E)$ where $\sigma_k(M)$ is the k-th largest singular value of M. Let $D = C^T C = V^{-1} \Lambda V$, $\Lambda = diag(1, \sigma_2(C), \ldots)$. **Theorem:** Let each of the r rounds of an interactive cipher have correlation matrix C then $\overline{I}(S) \leq \frac{1}{n-1} + ||C - E||^r$; also, $\overline{I}(S) \leq \frac{1}{n-1} + \sigma_2(C)^r$, $\sigma_2(C) \leq min\langle (1 - \sum_b min_a (C^T C)_{ab})^{\frac{1}{2}}, (1 - \sum_a min_b (C^T C)_{ab})^{\frac{1}{2}} \rangle$.

Let $\otimes$ be the Kroneker product. $\Phi(M,N) = \sum_{a,b} g_{ab} M^a \otimes N^b$, $\phi(x,y) = \sum_{a,b} g_{ab} x^a y^b$. The eigenvalues of $\Phi(M,N)$ are $\phi(\lambda_r(M), \lambda_s(N))$. if $C = A \otimes B$, the singular values of C are products of the singular values of A and B. The correlation of a non-keyed permutation $R = G \to G$ is $C = (F^* P F)(\overline{F^* P F})$ where $F = (f_{ab}))$, $f_{ab} = \frac{1}{\sqrt{n}} \chi^{-a}(b)$, $P = (p_{ab})$, $p_{ab} = \delta(a \oplus \phi(b))$. $C = U \cdot \overline{U}$ where U is unitary. **Theorem:** The correlation matrix of a keyed permutation $e_k : G \to G$ is $C = \frac{1}{|K|} \sum_k C^{(k)}$, $C^{(k)} = U^{(k)} \overline{U}^{(k)}, U^(k) = F P^{(k)} F^*$, $P^{(k)} = \delta(a \oplus e_k(b))$.

Dan's attack on RNGs:

```
s= IV;

NewRN() {
    t= s;
    s= b**t (mod p);
    r= q**t (mod p);
    output(r);
}
```

Suppose we know $e : q = b^e \pmod p$ then $r = b^{et} = (b^t)^e = s^e \pmod p$.

3.14 Related key attack on AES-256

Reminder: AES-128 has 10 rounds, AES-192 has 12 rounds and AES-256 had 14 rounds.

Birykov et al 9-Round attack on AES-256: Given two keys K_1, K_2 related by $K_2 = K_1 \oplus (b,b,b,b,a,0^{32},a,0^{32})$ (a,b) specified below and 2^{38} related plaintexts ($P_2 = P_1 \oplus (b,b,b,b)$), with each plaintext encrypted by each of the two related keys, we can find K_1, K_2 with work factor about 2^{39}.

Notation and key schedule: SB, SR, MC, and ARK are respectively the SubByte, shift-row, mix-column and add round-key transformations. Byte order for 32-bit input words is:

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

Suppose the 256 key is written as 8 32 bit words $W[0], \ldots, W[7]$, the first two round keys are $W[0], \ldots, W[3]$ and $W[4], \ldots, W[7]$. The remaining round keys are determined by:

```
for(i=8; i<60; i++) {
    if((i%8)==0)
        W[i]=W[i-8]^(SB,SB,SB,SB)W[i-1]+RCon(i/8);
    else if((i%8)==0)
        W[i]=W[i-8]^(SB,SB,SB,SB)W[i-1];
    else
        W[i]=W[i-8]^W[i-1];
}
```

8 round key trail for attack: Let $\alpha \to \beta$ be a differential that occurs through SB with probability 2^{-6}. Put $a = (\alpha, 0, 0, 0)^T$ and $b = MC((\beta, 0, 0, 0)^T)$. Rounds are numbered $0, 1, \ldots, 7$. $\delta = (b, b, b, b, a, 0, a, 0)$, $c = b \oplus SB(RotByte(a))$, $d = a \oplus SB(c)$, $e = d \oplus a$, $f = b \oplus c$. $\Delta(K^i)$ is the (xor) differenece of the subkey for round i and $\Delta(I^k)_{i,j}$ means the difference in the input to round k of bytes i and j.

Basic 8 **round differential:** $(b, b, b, b) \to (f, f, f, f), p = 2^{-54}$ can be constructed as follows: $P_1 = P_2 \oplus (b, b, b, b)$ and $\Delta(K^0) = (b, b, b, b)$. $\Delta(I^0) = 0^{128}$. At the end of round 0, the difference is 0^{128} and ARK at the end of round 0 adds a difference of $(a, 0, a, 0)$ which introduces two non-zero bytes with value α. Because of the differential, with $p = 2^{-12} = 2^{-6} \times 2^{-6}$, the difference becomes $(b, 0, b, 0)$ which is xored with the key differential $(b, 0, b, 0)$ yielding $\Delta(I^2) = 0$ with $p = 2^{-12}$. Similarly, given this difference, application of rounds $2, 3$ yield $\Delta(I^4) = 0$ with probability 2^{-12}. The combined probabililty that $\Delta(I^4) = 0$ is $p = 2^{-12} \times 2^{-12} = 2^{-24}$. The transition probability that $\Delta(I^4) = 0 \to \Delta(I^6) = (b, b, b, b)$ is 2^{-6} and $\Delta(I^6) = (b, b, b, b) \to \Delta(I^8) = (f, f, f, f)$ is 2^{-24}. Thus the plaintext differential $(b, b, b, b) \to (f, f, f, f)$ occurs with $p = 2^{-54}$.

Actual differentials used: By modifying the 8 round differentials, we get three truncated differentials: (1) By relaxing the conditions in round 7 and insisting that only byte 0 have difference 0, we get $\Delta(I^8_{0,1,2}) = 0, p = 2^{-36}$. (2) (the "Shifted Differential") By relaxing the conditions in round 7 and insisting that only byte 12 have difference 0, we get $\Delta(I^8_{13,14}) = 0, p = 2^{-36}$. (3) (the "Complemented Differential") By relaxing the conditions in round 5 in a 6 round differential and not imposing a condition on byte 5 (the others are 0), we obtain 16 possible differential outputs at the input to round 7. only byte 12 have difference 0, we get $\Delta(I^8_{13,14}) = 0, p = 2^{-36}$.

Full 9 **Round attack:**

1. Generate 2^{37} pairs $P' = P \oplus (b, b, b, b)$ and encrypt each P and P' with K and $K \oplus (b, b, b, b, a, 0, a, 0)$. Insert the cipher pairs (C, C') in a hash table indexed on $\Delta(C)_{0,10,13} = d_0, d_1, d_2$. Right pair has $\Delta(I^8_{0,1,2}) = 0$.

2. Guess K^8_{12} and partially decrypt to get $\Delta(I^8_{12})$. $\Delta(K^8_{12}) = d_0 \oplus \alpha$ is known.

3. Do same as 2 to d_0, d_1, d_2, K^8_{12} to get 6 bytes of K^8 $(2, 5, 6, 8, 9, 12))$.

4. For each remaining pair, guess c_3, d_3 and use SB on $(3, 7, 11, 15)$ of round 8 to suggest $K^8_{3,7,11,15}$.

5. Repeat with shifted differential.

6. By now, K^8 is known decrypt through round 7 then find K^7 as follows:
   (a) For right pairs, under main 8 round differential, guess $K^7_{0,4,8,12}$ and partially decrypt to get $\Delta(I^7_{0,4,8,12})$ discard when $\Delta(I^7_{0,4,8,12}) \neq (\alpha, \alpha, \alpha, \alpha)$. Right differences suggest right key values.
   (b) Use key schedule to get possible $K^7_{13,14,15}$.
   (c) Now $K^7_{0,4,8,13,14,15}$ is known. For 2^{26} to of the 238 pairs: Partially decrypt to get $\Delta(I^7_{0,1,4,6,8,11})$. Consider colums $0, 1, 2$ of $\Delta(I^7)$ separately and see if the differences of the two "known" bytes agree with the complementary differential. This filters 8 bits. Finally, for each of the remaining pairs, use $\Delta(I^7_{0,4,8,12})$ to retrieve full difference $\Delta(I^7)$. Then use the I/O differences though SB to suggest byte values for each byte of K^7 and discard bytes suggested less than 3 times. This should get the right key most times.

7. Now, K^7 and K^8 are known and we can run the key schedule backwards to get the key.

3.15 Trivium and Cube

Cube Attack: For any polynomial P and term t, write $P = tP_t + Q$, where the variables in P_t are disjoint from those in t and each term in Q misses at least one variable from t. P_t is called the *superpoly* of t in P. A *maxterm* of P is any product t of variables whose superpoly has degree 1 (i.e., is a linear or affine function which is not a constant). *Example:* $P(x_1, x_2, x_3, x_4, x_5) = x_1x_2x_3+x_1x_2x_4+x_2x_4x_5+x_1x_2+x_2+x_3x_5+x_5+1$. Let $t = x_1x_2$, $P(x_1, x_2, x_3, x_4, x_5) = x_1x_2(x_3 + x_4 + 1) + (x_2x_4x_5 + x_3x_5 + x_2 + x_5 + 1)$, the superpoly of x_1x_2 in P is $(x_3 + x_4 + 1)$.

Theorem: $\sum_t(tP_t + Q) = P_t$

Proof: $\sum_t Q = 0$ since every numerical value appears an even number of times. $\sum_t(tP_t + Q) = (\sum_t t)P_t$ since the only term in the sum that is non-zero is the one where all the variables are 1.

To apply in attack: For each candidate maxterm t, choose pairs of values for all the other variables X' and X''. Verify that the numerical values of the subcube sums satisfy the linearity test: $P_t(X') + P_t(X'') = P_t(X' + X'') + P_t(0)$. If the test succeeds multiple times, obtain the linear superpoly by checking the numeric effect of flipping each key bit x_i.

```
//  Trivium

//     Key size: 80 bits
//     IV size: 80 bits
//     State size: 288 bits
//     Up to 2^64 keystream bits

//     Step takes 15 bits and produces 3 new
//          state bits and 1 output bit.

Init()
{
    (s[1],..., s[93]):= (k[1],..., k[80],
                         0,...,0);
    (s[94], ..., s[177]):= (IV[1], ...,IV[80],
                            0, ...,0);
    (s[178], ..., s[288]):= (IV[1], ...,IV[80],
                             0, ...,0,1,1,1);
    for(i=1; i<= 4*288) {
        t1= s[66]+s[91]*s[92]+s[93]+s[171];   }
        t2= s[162]+s[175]*s[176]+s[177]+s[264];
        t3= s[162]+s[175]*s[176]+s[177]+s[264];
                                                    (s[1],..., s[93]):= (t3,s[1],...,s[92]);
                                                    (s[94],..., s[177]):= (t1,s[94],...,s[176]);
                                                    (s[178],..., s[288]):= (t2,s[178],...,s[288]);
                                                }
                                            }

                                            Step()
                                            {
                                                t1= s[66]+s[93];
                                                t2= s[162]+s[177];
                                                t3= s[243]+s[288];
                                                z= t1+t2+t3;
                                                t1+= s[91]*s[92]+ s[171];
                                                t2+= s[175]*s[176]+ s[264];
                                                t3+= s[286]*s[287]+ s[69];
                                                (s[1],..., s[93]):= (t3,s[1],...,s[92]);
                                                (s[94],..., s[177]):= (t1,s[94],...,s[176]);
                                                (s[178],..., s[288]):= (t2,s[178],...,s[288]);
                                                return (z);
```

Shamir and Dinur found 35 maxterms in the 767 round initialization.

Stream Cipher Notation: Input is $x(D) = x_0+x_1D+x_2D^2+\ldots$. Ourput is $y(D) = y_0+y_1D+y_2D^2+\ldots$. $f(x)$ is feedforward polynomial and $g(x)$ is feedback polynomial. $y(D) = \frac{f(D)}{g(D)}[x(D)+x^0(D)]+y^0(D)$ where $x^0 = D^{-m}(s \cdot g \pmod{D^m})$, $y^0 = D^{-m}(s \cdot f \pmod{D^m})$. $B = min_{\Gamma \neq 0}[w_h(\Gamma_Y) + w_h(M^T\Gamma_Y)]$. *Example:* The setup (left to right) at init is: $S_{box} \rightarrow \oplus \rightarrow 0 \rightarrow 0 \rightarrow$ feedforward tap $\rightarrow 1 \rightarrow$ feedback tap $\rightarrow 0 \rightarrow$

feedback tap $\rightarrow \oplus \rightarrow S_{box}$. $f(D) = D^4(D^{-2}+1)$, $g(D) = D^4(D^{-4}+D^{-1}+1)$, $s^0 = D$, $x^0(D) = D^{-3}$, $y^0(D) = D^{-1}$ then $y(D) = \frac{D^{-1}+D+D^2+D^4}{1+D^3+D^4} + D^{-1}$. $\gamma_x(D)$ is the input selection polynomial; $\gamma_x = q\frac{f^*}{(f^*,g^*)}$, $\gamma_y = q\frac{g^*}{(f^*,g^*)}$. $\gamma_y(D)$ is the output selection polynomial. $f^*(D) = f(D^{-1})$. $\gamma_x^* = \gamma_y^* \frac{f}{g}$; $\gamma_y = \gamma_x \frac{g^*}{f^*}$. In example, $\gamma_x(D) = 1+D+D^2+D^3$ and $\gamma_y(D) = 1+D^2+D^4+D^5$; $x_0+x_1+x_2+x_3 = y_0+y_2+y_4+y_5$. Let $d = (f_1^*f_2^*, g_1^*f_2^*, g_1^*g_2^*)$, $\gamma_u = q\frac{f_1^*f_2^*}{d}$, $\gamma_v = q\frac{g_1^*f_2^*}{d}$, $\gamma_w = q\frac{g_1^*g_2^*}{d}$, $\mathcal{W} = w_h(\gamma_u) + w_h(\gamma_v)$.

KeyLoq: 32-bit NLFSR, 64-bit rotating key, $NLF(a,b,c,d,e) = d+e+ac+ae+bc+be+cd+de+ade+ace+abd+abc$. $(e+b+a+y)\cdot(c+d+y) = 0$. Equations are: $L_i = P_i, 0 \le i \le 31$, $L_i = k_{(i-32) \pmod{64}} + L_{i-32} + L_{i-16} + NLF(L_{i-1}, L_{i-6}, L_{i-12}, L_{i-23}, L_{i-30}), 32 \le i \le 521$, $C_{i-528} = l_i, 528 \le i \le 559$. Degree reduction: $\alpha \leftarrow ab, \beta \leftarrow ae$. Define $f^{(i)}(x) = f^{(i-1)}(f(x))$. Keyloq equation is $E_k(P) = g_k(f_k^{(8)}(P)) = c$ where $f(x)$ is 64 rounds. Assume $f(x) = x, f(y) = y$ then we know 64 bits of input and output. Guess 16 bits of $g_k(x)$ key. Solve for 64 key bits plus 64 intermediate values. .26 of the keys have two fixed points.

Disk Encryption with ESSIV(cbc): $IV(\text{sector}) = Enc_{\text{salt}}(\text{sector})$, salt $= H(K)$.

CBC Padding attack: b bytes in a block. Number of values in a byte is W. Padding appends $n > 0$ bytes. For any block, y, want to compute last byte of $C^{-1}(y)$, where y is the block we're interested in decoding. Construct fake two block message $r||y$, $r = r_1, r_2, \ldots, r_b$, with r_i, random. If $r||y$ is valid, $C^{-1}(y) \oplus r$ ends with a valid pad. So last byte of $C^{-1}(y) = r_b \oplus 1$, most likely. Now replace r_b with $r_b \oplus 1$ and do next byte. Assume $a = a_1, a_2, \ldots, a_b = C^{-1}(y)$. Requires $O(NbW/2)$.

Permutation generating functions: Let $P(\pi, c_1, c_2)$ is the probability that π has c_1 one cycles and c_2 cycles of length $2, 4, 8$ then $P(\pi, c_1, c_2) = \frac{1}{c_1!c_2!}\frac{7}{8}^{c_2} e^{-15/8}$. $EGF = \frac{z^{c_1}}{(1-z)c_1!c_2!}[\frac{z^2}{2} + \frac{z^4}{4} + \frac{z^8}{8}]^{c_2} exp(\sum_{i|8} z^i/i)$. $\pi \in S_n, P(\pi \text{ has } c_1 \text{ fixed points}) = \frac{1}{e(c_1)!} = \frac{e^{-15/8}}{c_1!}e^{7/8}$. OGF: $C(z) = \sum_i z^i$, EGF: $C_e(z) = \sum_i \frac{c_i}{i!} z^i$. If $\mathcal{P}$ is the permutatation population generating function, $\mathcal{P}(x) = z + 2z^2 + 6z^3 + \ldots$ and $\mathcal{P}_e(x) = z + z^2 + z^3 + \ldots$. $1, 2, 3, 4$-selection generating function is $B(z) = 0 + z + z^2 + z^4$. For cycles, $\mathcal{C}_e(x) = z + \frac{z^2}{2} + \frac{z^3}{3} + \ldots = log(\frac{1}{1-z})$. Probability $\pi \in S_n$ does not have cycles of length k is $e^{-\frac{1}{k}}$.

3.16 Zero Knowledge Protocols

Some preliminaries first.

Theorem: If $n = pq$, and we know p, q, where p and q are primes then we can efficiently compute all four x: $y = x^2 \pmod{n}$.

> *Proof:* We can find x_p, x_q such that $y = {x_p}^2 \pmod{p}$ and $y = {x_q}^2 \pmod{q}$ using Tonelli-Shanks. Using the Chinese remainder theorem, we can compute t such that $t = x_p \pmod{p}$ and $t = x_q \pmod{q}$. Then $y - t^2 = 0 \pmod{p}$ and $y - t^2 = 0 \pmod{q}$ so $y = t^2 \pmod{n}$.

Theorem: Suppose $n = pq$, and we know n and the fact that p, q are primes. If we know n, y and all for $x : y = x^2 \pmod{n}$ then we can find p and q. then we can efficiently compute all x; $y = x^2 \pmod{n}$.

> *Proof:* Suppose the square roots of y are $\pm a$ and $\pm b$. $y^2 = (ab)^2 \pmod{n}$, so $(y-ab)(y+ab) \mid n$. We can find, say p by computing $(y-ab, n)$.

Coin flipping protocol: Alice picks p, q and computes $n = pq$. Protocol is:

1. Alice $\rightarrow$ Bob: n.
2. Bob calculates $y = x^2 \pmod{n}$ using a random x. Bob $\rightarrow$ Alice: y.
3. Alice calculates all four square roots, $\pm a$, $\pm b$. She picks one, say b, and sends it to Bob. Alice $\rightarrow$ Bob: b.
4. Alice wins if $x = \pm b$ and loses if $x \neq \pm b$. Bob sends her a message telling her whether she won or lost.

Alice can check Bob isn't cheating because if $x = \pm a$, Bob knows all four square roots $\pmod{n}$ and can tell Alice p, q.

Zero knowledge secret proof: Peggy knows a secret, s, and want to prove she know is to Victor without revealing it. Peggy finds a p, q and computes $n = pq$ and $y = s^2 \pmod{n}$ and checks that $(y, n) = 1$. She chooses r_1 at random and computes $r_2 = s{r_1}^{-1} \pmod{n}$ Note that $s = r_1 r_2 \pmod{n}$. Finally, Alice computes $x_1 = (r_1)^2 \pmod{n}$ and $x_2 = (r_2)^2 \pmod{n}$. Protocol is:

1. Peggy $\rightarrow$ Victor: n, y, x_1, x_2.
2. Victor checks that $y = (x_1 x_2)^2 \pmod{n}$, and choses one, say x_1. Victor $\rightarrow$ Peggy: x_1.
3. Peggy $\rightarrow$ Victor: r_1.
4. Victor confirms that $(r_1)^2 = x_1 \pmod{m}$.

Without knowing s, Peggy succeeds with probability $\frac{1}{2}$ but always succeeds if she knows s. Repeating this m times, Victor knows that Peggy knows s with probability $1 - (\frac{1}{2})^2$.

More efficient proof of secret knowledge protocol (FFS): Again, Peggy finds a p, q and computes $n = pq$. There are k secrets $s_1, s_2, \ldots s_k$. Peggy picks r at random and computes $x = r^2 \pmod{n}$. She also computes $v_i = s_i^2 \pmod{n}$ for $i = 1, 2, \ldots, k$.

1. Peggy $\rightarrow$ Victor: $n, x, v_1, v_2, \ldots, v_k$.
2. Victor picks k values $b_i \in \{0, 1\}$. Victor $\rightarrow$ Peggy: $b_1, b_2, \ldots, b_k$.
3. Peggy computes $y = r s_1^{b_1} s_2^{b_2} \ldots s_k^{b_k} \pmod{n}$.
4. Victor checks that $x = y^2 v_1^{b_1} v_2^{b_2} \ldots v_k^{b_k} \pmod{n}$.

As before, repeat this as often as you like.

Secret splitting: Suppose we want to share a secret, s, among n people, so that and t of them could assemble the secret. Pick $p > s$ and choose $s_1, s_2, \ldots, s_{t-1}$ at random $0 \leq s_i < p$. Put $s_0 = s$ and form $f(x) = s_0 + s_1 x + \ldots + s_{t-1} x^{t-1}$. Now chose $x_1, x_2, \ldots, x_n$ at random $0 \leq x_i < p$ and put $y_i = f(x_i) \pmod{p}$. Give (x_i, y_i) to participant i. Any t participants can find $s = s_0$.

Chapter 4

Physics

4.1 Basic Laws

Classical Physics: $\vec{F} = \frac{d\vec{p}}{dt}$, $\vec{p} = m\vec{v}$, $m = \frac{m_0}{\sqrt{1-(\frac{v}{c})^2}}$, $F = -G\frac{m_1 m_2}{{r_{12}}^2}$. For conservative forces, there is a potential function $U(x, y, z)$ and the force in w direction is $F = -\frac{\partial U}{\partial w}$. $\vec{F} = q(\vec{E} + \vec{v} \times \vec{B})$. $E = -\nabla V$ (V corresponds to work done by E per unit charge or U/q).

Special Relativity: Primed (') coordinate system is moving at constant velocity u in the x direction with respect to the unprimed system; put $\gamma = \frac{1}{\sqrt{1-\frac{u^2}{c^2}}}$. The *Lorentz transform* is $x' = \gamma(x - ut)$, $y' = y$, $z' = z$, $t' = \gamma(t - \frac{ux}{c^2})$. Newton's law, $F = \frac{dp}{dt}$, remains invariant under the Lorentz transform, that is, $\frac{dp}{dt} = \frac{dp'}{dt'}$. Maxwell's equations are also invariant under the Lorentz transform. The energy-momentum four-vector is (cp_x, cp_y, cp_z, E) and its squared length is $(cp_x)^2 + (cp_y)^2 + (cp_z)^2 - E^2$. It transforms like $p'_x = \gamma(p_x - E\beta/c)$, $p'_y = p_y$, $p'_z = p_z$, $E' = \gamma(E - \beta c p_x)$, where $\beta = \frac{u}{c}$. The length of the energy-momentum four-vector is invariant under the Lorentz transform. $E^2 - (pc)^2 = (m_0 c^2)^2$.

Maxwell's Equations (MKS): $\nabla \cdot \vec{j} = -\frac{\partial \rho}{\partial t}$, $\nabla \cdot \vec{E} = \frac{\rho}{\epsilon_0}$, $\nabla \times \vec{E} = -\frac{\partial \vec{B}}{\partial t}$, $\nabla \cdot \vec{B} = 0$, $c^2 \nabla \times \vec{B} = \frac{j}{\epsilon_0} + \frac{\partial \vec{E}}{\partial t}$, $c = \frac{1}{\sqrt{\mu_0 \epsilon_0}}$. $S = \epsilon_0 c^2 E \times B$.
In *non-dispersive media*, $\vec{D} = \epsilon\vec{B}$ and $\vec{H} = \mu\vec{B}$.

Maxwell solution outline: Maxwell's equations give $\nabla \times (E + \frac{\partial A}{\partial t}) = 0$, choosing gauge $\nabla \cdot A = -\frac{1}{c^2}\frac{\partial \phi}{\partial t}$, we get $\nabla^2\phi - \frac{1}{c^2}\frac{\partial^2 \phi}{\partial t^2} = -\frac{\rho}{\epsilon_0}$. We obtain a similar equation in terms of A and j . Both are of the form

$$\nabla^2 \psi(r, t) - \frac{1}{c^2}\frac{\partial^2 \psi}{\partial t^2} = -s$$

Let $r^2 = x^2 + y^2 + z^2$. $\nabla^2\psi(r) = \psi''(r) + \frac{2}{r}\psi'(r)$ or $\nabla^2\psi = \frac{1}{r}\frac{d^2}{dt^2}(r\psi)$. If $s = 0$, $\frac{d^2}{dr^2}(r\psi) - \frac{1}{c^2}\frac{\partial^2}{\partial t^2}(r\psi) = 0$ and the solution is $\psi(r, t) = \frac{f(t-\frac{r}{c})}{r}$. Recall electrostatic analogy: $\nabla^2\phi = -\frac{\rho}{\epsilon_0}$, then $\phi = \frac{1}{4\pi\epsilon_0}\frac{q}{r}$ where $q = \int \rho dV$. Thus $\psi(r, t) = \frac{f(t)}{r}$ as $r \to 0$. If $S(t) = \int s(t)dV$ and ψ satisfies $\nabla^2\psi = -s$ as $r \to 0$ then ψ satisfies $\nabla^2\psi - \frac{1}{c^2}\frac{\partial^2}{\partial t^2}\psi = -s$. We have $\psi(x, y, z, t) = \frac{1}{4\pi}\frac{S(t-r/c)}{r}$. So for a small lump of charge, $d\psi(r, t) = \frac{1}{4\pi\epsilon_0}\frac{\rho(2, t-r_{12}/c)}{r_{12}}dV_2$. For small charges travelling at velocity v, $\psi(r, t) = \frac{1}{4\pi\epsilon_0}\frac{q}{r'_{12}}\frac{1}{1-v_{r'}/c}$. Solving

gives Feynman's solution, $E = \frac{-q}{4\pi\epsilon_0}(\frac{e_{r'}}{r'^2} + \frac{r'}{c}\frac{d}{dt}\frac{e_{r'}}{r'^2} + \frac{1}{c^2}\frac{d^2}{dt^2}(e_{r'}))$, $E = cB$. $A' = A + \nabla\psi$ $\phi' = \phi - \frac{\partial\psi}{\partial t}$ is a *gauge transformation.* Solving equations produces $\phi(1,t) = \int \frac{\rho(2,t-(r/c))}{4\pi\epsilon_0 r_{12}} dV$, and $A(1,t) = \int \frac{j(2,t-(r/c))}{4\pi\epsilon_0 c^2 r_{12}} dV$. $\phi(1,t) = \frac{q}{4\pi\epsilon_0 r'(1-\frac{v_{r'}t}{c})}$ (*Lenart-Weichart*) at high velocities.

Waves in conductor: For a conductor, $\rho = 0$ and $J = \sigma E$. $\nabla \times (\nabla \times \vec{E}) = -\frac{\partial(\nabla\times\vec{B})}{\partial t}$. $\nabla \times (\nabla \times E) = \nabla(\nabla \cdot E) - \nabla^2 E$, and $-\frac{\partial(\nabla\times\vec{B})}{\partial t} = -\frac{1}{c^2}(\frac{\sigma}{\epsilon}\frac{\partial E}{\partial t} + \frac{\partial^2 E}{\partial t^2})$. Apply trial solution $E = E_0 e^{i(\omega t - k\cdot r)}$ and get $-k^2 - i\omega\mu\sigma + \omega^2\mu\epsilon = 0$. Putting $k = \alpha - i\beta$, we get $\alpha = \omega\sqrt{\mu\epsilon}(\frac{1}{2} + \frac{1}{2}\sqrt{1 + \frac{\sigma^2}{\omega^2\epsilon^2}})$ and $\beta = \frac{\omega\mu\sigma}{2\alpha}$. So, $E = E_0 e^{i(\omega t - \alpha\cdot r)} e^{-\beta\cdot r}$. For copper, $\sigma \approx 5.76 \times 10^7 (\Omega - m)^{-1}$).

Radiation from point charge: For a, charge q, accelerating at $\vec{a}(t')$, $t' = t - r/c$, at low velocity, $E_{rad}(\vec{r},t) = -\frac{1}{4\pi\epsilon_0 c^2}\frac{q}{r}\vec{a}_\perp(t')$. $cB = E$ and $|S| = \frac{1}{\mu_0}|E \times B|$ so $|S| = \frac{1}{16\pi^2\epsilon_0 c^3}\frac{q^2}{r^2}|\vec{a}(t')|^2 sin^2(\theta(t'))$. Since $dP(r,t) = |S|dA$, the total radiated power is $P(t) = \frac{a^2(t')q^2}{4\pi\epsilon_0 c^3}\int_{sphere}\frac{1}{4\pi r^2} sin^2(\theta(t'))dA$. $\frac{dA}{4\pi r^2} = sin(\theta)d\theta d\phi$ in polar coordinates. So $P(t) = \frac{1}{4\pi\epsilon_0 c^3} q^2 a^2(t') \overline{sin^2(\theta(t'))}$ where $\overline{sin^2(\theta(t'))} = \int_{sphere} sin^2(\theta)\frac{dA}{4\pi r^2}$. $\int_{sphere} |sin(\theta)|^3 d\theta d\phi = \frac{2}{3}$ so $P(t) = \frac{2}{3}\frac{\mu_0}{4\pi c} q^2 a^2(t')$.

Oscilating dipole: $\vec{p} = q\vec{d}$. The dipole consists of a charge $+q$ and a charge $-q$ separated by a distance, d where d is much smaller than the wavelength. At low speed, $A(1,t) = \frac{1}{4\pi\epsilon_0 c^2}\frac{1}{r}\int v\rho(2, t - r/c)dV_2 = \frac{vq}{r} = \frac{\dot{p}(t-r/c)}{4\pi\epsilon_0 c^2 r}$. $\nabla \times A = B$, $B_x = \frac{\partial A_z}{\partial y}$ and $B_y = -\frac{\partial A_z}{\partial x}$. $B_x = \frac{1}{4\pi\epsilon_0 c^2}[\dot{p}\frac{\partial\frac{1}{r}}{\partial y} + \frac{1}{r}\frac{\partial\dot{p}}{\partial y}] = -\frac{1}{4\pi\epsilon_0 c^2}[\frac{y}{r^3}\dot{p} + \frac{y}{cr^2}\ddot{p}]$. Use $\nabla \cdot A = -\frac{1}{c^2}\frac{\partial\psi}{\partial t}$. Then $\frac{\partial\psi}{\partial t} = c^2\nabla \cdot A = \frac{d}{r}\frac{1}{4\pi\epsilon_0} - [\frac{1}{r^2}I(t - r/c) + \frac{1}{rc}I'(t - r/c)]\frac{\partial r}{\partial z}$, $r^2 = x^2 + y^2 + z^2$. $\psi = \frac{dz}{4\pi\epsilon_0}[\frac{q(t-r/c)}{r^3} + \frac{I(t-r/c)}{r^2 c}]$.

Poynting: $dW = F \cdot ds = \int_Q dq(E + v \times B) \cdot vdt$. $\frac{dW}{dt} = \int_{V_0}(E \cdot v)\rho dV = \int_{V_0} E \cdot jdV$. Substitute $j = \epsilon_0(c^2\nabla \times B - \frac{\partial E}{\partial t})$ and use $A \cdot \nabla \times B = B \cdot \nabla \times A - \nabla \cdot (A \times B)$ to get $\frac{dW}{dt} = -\int_{v_0} \epsilon_0 c^2 \nabla \cdot (E \times B) - \frac{1}{2}\epsilon_0\frac{\partial}{\partial t}\int_{V_0} E^2 dV - \frac{1}{2}\epsilon_0 c^2\frac{\partial}{\partial t}\int_{V_0} B^2 dV$.

Fundamental constants: $G = 6.671 \times 10^{-11}\frac{Nm^2}{kg^2}$, $c = 2.99725 \times 10^{10}\frac{cm}{s}$, $k_B = 1.38 \times 10^{-16}\frac{ergs}{deg}$, $h = 6.6262 \times 10^{-27} erg - sec$, $q_e = 1.60219 \times 10^{-19} C$, $\epsilon_0 = 8.854 \times 10^{-12}\frac{C^2}{N-m^2}$, STP: $22.4 \times 10^3\frac{cm^3}{mol}$, $R = 8.3143\frac{J}{mol-deg}$, $N_0 = 6.022 \times 10^{23} mol^{-1}$.

Some consequences of Maxwell: *EMF* is the total accumulated force through wire, ($\mathcal{E} = -\frac{d\phi_B}{dt}$).
For conservative electric field: $\Delta\phi = -\int_a^b qEds$, $\Delta V = \frac{\Delta\phi}{q}$. *Coulomb:* $F = \frac{1}{4\pi\epsilon_0}\frac{q_1 q_2}{r^2}\hat{r}$. *Gauss (always):* $\Phi_E = \int_S E \cdot dA = \frac{q_{in}}{\epsilon_0}$, S, closed. $\Phi_B = \int_S B \cdot dA = 0$, S, closed. *Biot-Savart (steady currents):* $B = \frac{\mu_0}{2\pi}\frac{qv\times e_r}{r^2}$. *Ampere:* $\int_C B \cdot dl = \mu_0(I_{enclosed} + \epsilon_0\frac{d\Phi_E}{dt})$. *B for wire (steady currents only):* $B = \frac{\mu_0 I}{2\pi r}$. *Faraday:* $\mathcal{E} = \int_C E \cdot dl = -\frac{d\Phi_B}{dt}$. $E = 0$ for conductor in *electrostatics.* $C = \kappa_0 C_0$. Steady current in conductor: $J = nqV_d = \sigma E$, $E = \rho J$.
AC: $V = IZ$. *Induced currents* gives rise to induced EMF ($\mathcal{E} = -\frac{d\Phi_B}{dt}$). *Pointing vector* describes energy flow $S = \frac{1}{\mu_0}E \times B$; transmitted power is $P = \int S \cdot dA$. $\frac{S}{c}$ is the *radiation pressure. Displacement currents*, like the initial current to charge a capacitor, also gives rise to fields. *Energy density* is $u = \frac{1}{2}\epsilon_0 E^2 + \frac{1}{2\mu_0}B^2$. *Rayleigh-Jeans:* $B_\nu(T) = \frac{2kT\nu^2}{c^2}$.

Antennas and Propagation $L_S = 32.4 + 20log(f_{MHz}) + 20log(d_{km})$. *Friis Formula*: $P_R = \frac{P_T G_T G_R \lambda^2}{(4\pi R)^2}$. *Effective aperture:* $A_e = \frac{\lambda^2}{4\pi}G$.

Oscillating Dipole (Antenna): $E = \frac{p_0 k^2}{4\pi\epsilon_0}\frac{sin(\theta)}{r}sin(\omega t - kr)$, $E = cB$.

Magnetism and relativity: Let $S(x, y, z, t)$ be the reference frame of a stationary wire with center line along the y axis and cross section A. Suppose there is a negative charge, q at a distance, r, in the z direction moving at a velocity v_0 parallel to the y axis. Suppose the wire has heavy positively charged particles of density ρ_+ which are stationary and free electrons of density ρ_- moving in the positive y direction with velocity, v, giving rise to a current, I in the $-y$ direction. Overall, the wire is electrically neutral, so, $\rho_+ = \rho_-$. The current generates a $B = \frac{\mu_0 I}{2\pi r}$ and the charge, q thus experiences a force $F = qv_0 \times B = \frac{1}{4\pi\epsilon_0 c^2}\frac{2qvv_0}{r} = \frac{1}{4\pi\epsilon_0 c^2}\frac{2\rho_- Aqvv_0}{r}$. Now let $v_0 = v$ and we get $F = \frac{q}{2\pi\epsilon_0 c^2}\frac{\rho_- A}{r}\frac{v^2}{c^2}$. Now let $S'(x', y', z', t')$ be the reference frame moving in the positive y direction with velocity v. In this frame, q is not moving (so there is not force due to the magnetic field) and the heavy positive charges are moving to the left with velocity v (so again there is a current I to the left). However, the wire is forshortened: $L' = L\sqrt{1 - \frac{v^2}{c^2}}$ so the charge density $\rho'_+ = \frac{\rho_+}{\sqrt{1-\frac{v^2}{c^2}}}$ and, since the electrons are now "at rest", they have their rest density, so $\rho'_- = \rho\sqrt{1 - \frac{v^2}{c^2}}$. So $\rho' = \rho_+ + \rho_- = (\rho_+)(\frac{v^2}{c^2})\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}$ and q experiences an electric field $E' = \frac{1}{2\pi\epsilon_0}\frac{A\rho_+(\frac{v^2}{c^2})}{r\sqrt{1-\frac{v^2}{c^2}}}$ towards the wire. Thus $F' = F\frac{1}{\sqrt{1-\frac{v^2}{c^2}}}$ which is exactly how F would transform under the Lorentz transformation. In other words, the magnetic force, F, in S, transforms to a corresponding electric force, F', in S' with same value as F, relativistically corrected.

Magnetic substances: Some materials have microscopic current loops that give rise to magnetic fields in substances. *Diamagnetic* materials have no microscopic loops but external field causes loops, these materials make fields a little weaker. *Paramagnetic* materials make fields a little stronger (some aligned loops). *Ferromagnetic* materials make fields a lot stronger (aligned loops).

Devices: $\Phi_B = Li$, $\mathcal{E} = -L\frac{di}{dt}$. $U = \frac{1}{2}CV^2$. $U = \frac{1}{2}LI^2$. $Iz = V$. $Z_C = \frac{1}{i\omega C}$, $Z_L = i\omega L$, $Z_R = R$.
Mutual Inductance: $\mathcal{E}_2 = -M\frac{di_1}{dt}$, $\mathcal{E}_1 = -M\frac{di_2}{dt}$. $U_L = \frac{1}{2}LI^2$, $U_C = \frac{1}{2}CV^2$.
Kirchoff: $\sum_k v_k = 0$, k covers loop; $\sum_k i_k = 0$, k covers node.
Thevinen equivalence: Two terminal linear network is equivalent to voltage source V_{Th} and impedance in series.
Norton equivalence: Two terminal linear network is equivalent to current source V_N and conductance G_N in parallel.
Resistor: $R = \frac{\rho L}{A}$, $\rho = \rho_0(1 + \alpha\Delta T)$. *Battery:* $\mathcal{E} - Ir_{internal} = V_{ab}$.
$S/N = 1 - log_{10}(\frac{P_S}{P_N})$. $60dB$ is hi-fi, $90dB$ for CD, Ear detects $120dB$.
Johnson noise: $N = kTB$, $B =$ bandwidth. *Phasor:* $v = a + bi$, $|v| = \sqrt{a^2 + b^2}, tan(\phi) = \frac{b}{a}$.
Low-pass (Inductance in series, capacitance across EMF), for *high-pass* switch capacitance and inductance.
Low pass transfer: $\frac{V_{out}}{V_{in}} = \frac{1}{\sqrt{1+\omega^2 R^2 C^2}}$. *High pass transfer:* $\frac{V_{out}}{V_{in}} = \frac{1}{\sqrt{1+\frac{R^2}{\omega^2 C^2}}}$.
Reactive: no real term; *dissipative:* real term > 0.
Transmission line: $\frac{\partial^2 I}{\partial x^2} = L_0 C_0 \frac{\partial^2 I}{\partial t^2}$; impedance is $z_0 = \sqrt{\frac{L_0}{C_0}}$. *Propagation factor:* $\alpha = \frac{V_{n+1}}{V_n}$.
Channel Capacity: $C = Blg(1 + S/N) \to \frac{B(S/N)}{kT}$.
Antenna: $\frac{P_R}{P_T} = \frac{A_T A_R}{\lambda^2 L^2}$. *Antenna efficiency* $= \frac{R_R}{R_R + R}$. $ERP = TPO \times gain$.
Bipolar transistor $i_c = \beta i_b$, $i_b = \frac{v_b}{(\beta+1)r_e}$. $V_t = \frac{kT}{q} \approx 25mA$. $r_e = \frac{kT}{qi_c}$. $i_c = i_{cs}(e^{\frac{qv_{be}}{kT}} - 1)$.
FET transistor $g_m = \frac{\Delta i_{DS}}{\Delta v_{gs}}$. $i_D = i_{DSS}(1 - \frac{V_{sg}}{V_P})^2$.
Impedance matching and power transfer: $\rho = \frac{Z_L - Z_0}{Z_L + Z_0}$, $SWR = \frac{1+\rho}{1-\rho} = \frac{Z_L}{Z_0}$, $\frac{P_{ref}}{P_{trans}} = (\frac{Z_L - Z_0}{Z_L + Z_0})^2$, $\rho =$

$\sqrt{\frac{P_{reflected}}{P_{transmitted}}}$.

Op Amp: $v_o = A_{OL}v_d$. Transfer and two terminal input and output. Op amp rules: (1) No current into op amp and (2) with negative feedback $V_+ = V_-$. $R_i \approx 10^4\Omega$, $A \approx 10^5$, $R_L \approx 10^3\Omega$.

Channel capacity: $C = Blg(1 + \frac{S}{N})b/s$.
Circuits: $X_C = -\frac{j}{\omega C}$, $V_C = X_C I_C$, $X_L = j\omega L$, $V_L = X_L I_L$, $Q = \frac{X}{R}$, $BW = \frac{f_0}{Q_u} = \frac{f_0}{\Delta f}$.
Capacitor: $q(t) = CV_{max}(1 - e^{-\frac{t}{RC}})$.
Inductor: $i(t) = i_{max}(1 - e^{-\frac{t}{LR}})$.
$R_{Th} = \frac{v_{oc}}{i_{sc}}$. For RLC with $R = .09\Omega$, $L = 5\mu F$, $C = 6.693nF$, $\omega_0 = \frac{1}{\sqrt{LC}} = 5.4 \times 10^6/sec$, $f = 870$ kHz, $\Delta f = 2.9$ kHz, $Q = 300$.
Transformer: $\frac{V_S}{V_P} = \frac{N_S}{N_P}$.
Integrator: $v_o = -\frac{1}{R_1 + R_L}\int_0^t v_i dt$.
Bipolar model: $r_\pi = \frac{kT}{qI_B} \approx 5.4k\Omega$, $i_c = \beta i_b$, $v_{be} = i_b r_\pi$, $i_c = -\alpha i_E$, $\frac{di_B}{dv_{bc}} = \frac{1}{r_\pi}$, $I_e = I_C + I_B = (h_{FE} + 1)I_B$. $i_b = \frac{I_{ES}}{\beta+1}exp(\frac{qv_{BE}}{kT})$, $v_{be} \approx .7V$ for Si. At $300K$, $\frac{kT}{q} \approx .026V$. Saturation for Si $|v_{CE}| \approx 0.2V$, $|v_{BC}| \approx 0.5V$.
Parameters: $h_{ie} = \frac{\partial v_{BE}}{\partial i_B}$, $h_{fc} = \frac{\partial i_C}{\partial i_B}$. For simple amp, $\frac{v_0 - v_A}{R_L} - \frac{v_A}{R_2} - \beta i_1 = 0$ and $A_{oc} = \frac{-\beta R_C}{r_\pi}$, $R_1 = 3M\Omega$, $R_C = 10k\Omega$. $v_{CC} \approx 15v$, $G_v = \frac{AR_L}{R_0 + R_L}$. $|A_{max}| = \frac{V_{cc}}{\frac{kT}{q}}$, frequency response is $-\beta R_C v_s \frac{1 + j\omega C_1 R_C}{[r_\pi + (1+\beta)R_E] + j\omega C_1 r_\pi R_E}$.
FET: $g_m = \frac{\Delta i_{DS}}{\Delta V_{GS}}$.

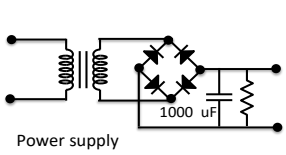
Common emitter: $A_V = \frac{R_c}{R_e}$. Design: (1) Choose v_{cc} (say $12V$), and $A_V = 5$, (2) choose Q point $i_{ceq} = 4mA$, $v_{be} = .7V$, $v_{ceq} = 5V$ (guide is $\frac{V_{cc}}{2}$). Finally, suppose $\beta = 150$. Calculate $R_c + R_e = \frac{v_{cc} - v_{ceq}}{i_{ceq}} = 1.75k\Omega$. Since $R_c = 5R_e$, $R_e = 270\Omega$ and $R_c = 1.5 \times 10^3\Omega$. $i_b = \frac{v_{ceq}}{\beta} = 27\mu A$. Pick current through R_1 and R_2 (guide is $10i_b$) of $270\mu A$. $V_{R_2} = .7 + i_{ceq}R_e = 1.8V$ and $V_{R_1} = 10.2V$, $R_2 = \frac{1.8V}{270\mu A} = 6.7k\Omega$, $R_1 = \frac{5.3V}{270\mu A} = 38 \times 10^3\Omega$. $Z_{in} = R_1||R_2||(\beta + 1)r_e \approx (\beta + 1)r_e$, $Z_{out} \approx R_c$. $r_3 \approx 1K\Omega$.

Common collector (emitter follower): Design: $\beta = 150$ as before, $A_V = 1$. (1) Choose v_{cc} (say $12V$), (2) choose Q-point: $i_{ceq} = 5mA$, $v_{ceq} = 6V$ (guide is $\frac{v_{cc}}{2}$), $v_{be} = .7V$, and $i_{R_1 - R_2} = 10i_b$. $v_{cc} = v_{be} + i_{ceq}R_e$, $R_e = 1.2k\Omega$. $i_b = \frac{i_{ceq}}{\beta} = 33\mu A$. $i_{R_1 - R_2} = 10i_b = 330\mu A$. $v_{R_2} = v_{be} + i_c R_e = .7 + 5mA(1.2 \times 10^3\Omega) = 6.7V$, $v_{R_1} = 5.3V$. $R_2 = \frac{6.7}{330\mu A} = 20 \times 10^3\Omega$, $R_1 = \frac{5.3}{330\mu A} = 16k\Omega$. $\frac{1}{Z_{in}} = \frac{1}{R_1} + \frac{1}{R_2} + \frac{1}{R_e(\beta+1)}$. $Z_{in} = R_1||R_2||(\beta + 1)r_e$, $Z_{out} = R_e||r_e$. $R_{in} = 50$ and $Z_{out} = 5\Omega$.

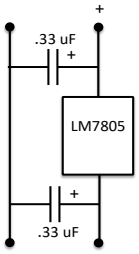
Common base: $A_V = \frac{R_C||R_L}{r_e}$. Design: Select $V_{cc} = 12V$ and $R_e = 50\Omega$,$V_{be} = .7V$, $R_L = 10^3\Omega$, $i_{ceq} = 5mA$, $v_{ceq} = 6V$. $i_b = \frac{i_{ceq}}{\beta} = 33\mu A$. Current through R_1, R_2 is $10i_b = 330\mu A$. $v_{R_2} = v_{be} + i_c R_e = 6.7V$, $V_{R_1} = 5.3V$. $R_2 = 20 \times 10^3\Omega$, $R_1 = 16 \times 10^3\Omega$. $v_{R_c} = \frac{(v_{ceq} - i_{cq}R_e - v_{ceq})}{i_{ceq}}$, $R_c = \frac{v_{R_c}}{i_{ceq}} \approx 1.35 \times 10^3\Omega$. $A_V = \frac{1.5 \times 10^3 || 10^3}{r_e} = 118$ $Z_{in} = R_e||(\beta + 1)r_e$, $Z_{out} \approx R_c$.

π-network: $X_{C_1} = \frac{R_{in}}{Q}$, $X_L = \frac{QR_{in} + \frac{R_{in}R_{out}}{X_{C_2}}}{Q^2 + 1}$. $R_{in} = 300$, $R_{out} = 50$, $F_C = \sqrt{7.7 \times 6.6}$, $BW = 1.1$ MHz, $Q = \frac{7.13}{1.1} = 6.48$, $Q^2 + 1 = 43 > \frac{300}{50}$, $X_{C_1} = 46.3\Omega$, $X_{C_2} = 20.1\Omega$, $X_L = 62.5\Omega$.

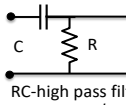
Signal processing: h_n is impulse response to $\delta(0)$ at time step n. $X(\omega) = \sum_{n=-\infty}^{\infty} x(n)e^{-j\omega n}$; $x_n = \frac{1}{2\pi}\int_{-\pi}^{\pi} X(\omega)e^{j\omega n}d\omega$. *Frequency response:* $H(\omega) = \sum h_n e^{-j\omega n}$. $X(z) = \sum x_n z^{-n}$; $x_n = \frac{1}{2\pi j}\int_S X(z)z^{n-1}dz$.



Power supply

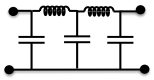


Voltage regulator

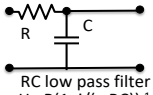


RC-high pass filter

$H = (1 - \frac{j}{\omega RC})^{-1}$

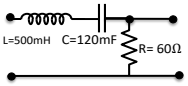


Line filter



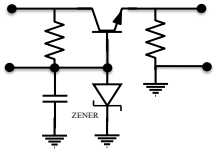
RC low pass filter

H= R(1+j/(wRC))$^{-1}$

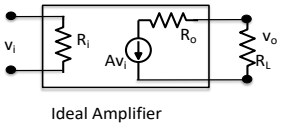


RC Band-pass filter

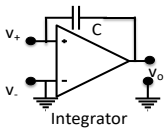
H= R(R+j(wL-1/(wC)))$^{-1}$



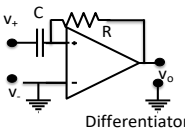
Voltage regulator



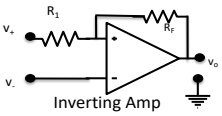
Ideal Amplifier



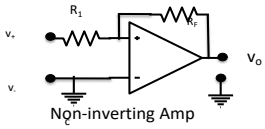
Integrator



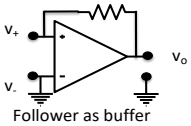
Differentiator



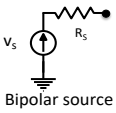
Inverting Amp



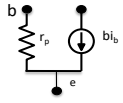
Non-inverting Amp



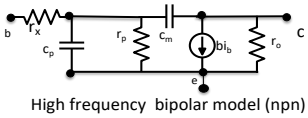
Follower as buffer



Bipolar source model

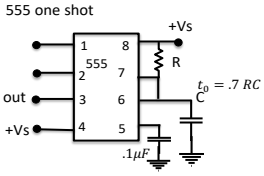


Simple bipolar model

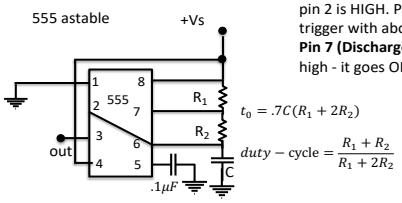


High frequency bipolar model (npn)

555 one shot



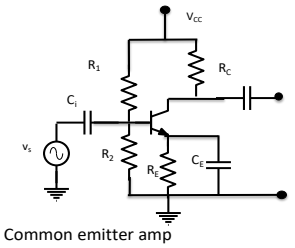
555 astable



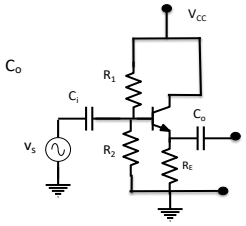
Pin 1: -Vs
Pin 8: +Vs
Pin 2 (Trigger): Out HIGH if V < V_{CC}/3. Pin 2 controls pin 6. If pin 2 is LOW, and pin 6 LOW, output goes and stays HIGH. If pin 6 HIGH, and pin 2 goes LOW, output goes LOW while pin 2 LOW. Pin 2has a very high impedance (about 10M) and will trigger with about 1uA.
Pin 3 (Output): (Pins 3 and 7 are "in phase.") Goes HIGH (about 2v less than rail) and LOW (about 0.5v less than 0v) and will deliver up to 200mA.
Pin 4 (Reset): Internally connected HIGH via 100k. Must go below 0.8v to reset the chip.
Pin 5 (Control): voltage applied to this pin will vary the timing of the RC network (quite considerably).
Pin 6 (Threshold): HIGH if > 2 V_{CC}/3, make output LOW only if pin 2 is HIGH. Pin 6 has very high impedance (~10M) and will trigger with about 0.2uA.
Pin 7 (Discharge): Pin 7 is equal to pin 3 but pin 7 does not go high - it goes OPEN. When LOW it sinks about 200mA.

324 op amp

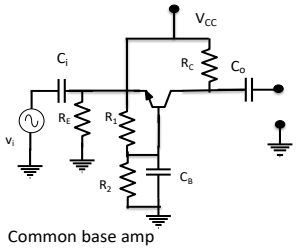
1 (o1)	(o4) 14
2 (i1-)	(i4-) 13
3 (i1+)	(i4+) 12
4 (V+)	(GND) 11
5 (i2+)	(i3-) 10
6 (i2-)	(i3+) 9
7 (o2)	(o3) 8



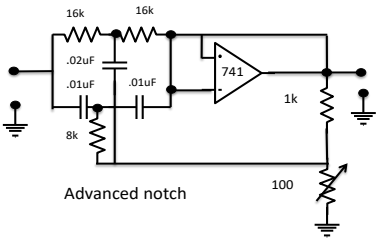
Common emitter amp



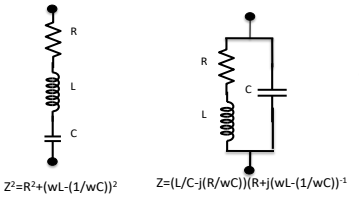
Common collector amp (Emitter Follower)

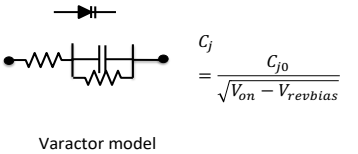


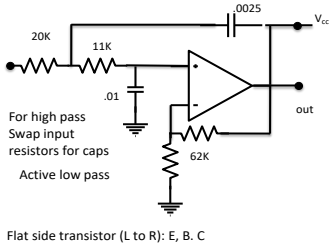
Common base amp

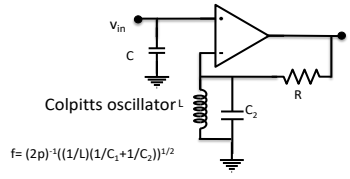


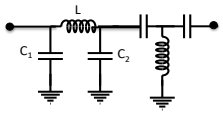
Advanced notch











SN74LS00

1 (A)		(V+)	14
2 (B)		(A)	13
3 (Y)		(B)	12
4 (Y)		(Y)	11
5 (B)		(Y)	10
6 (A)		(B)	9
7 (Gnd)		(A)	8

4 NAND

SN74LS02

1 (Y)		(V+)	14
2 (A)		(Q)	13
3 (B)		(!Q)	12
4 (Y)		(C)	11
5 (A)		(R)	10
6 (B)		(K)	9
7 (Gnd)		(J)	8

4 NOR

SN74LS06

1 (A)		(V+)	14
2 (!A)		(D)	13
3 (B)		(!!D)	12
4 (!B)		(E)	11
5 (C)		(E!)	10
6 (!C)		(F)	9
7 (Gnd)		(!F)	8

6 Inverter

SN74LS10

1 (A1)		(V+)	14
2 (A2)		(A3)	13
3 (C1)		(AO)	12
4 (C2)		(B3)	11
5 (C3)		(B2)	10
6 (CO)		(B1)	9
7 (Gnd)		(BO)	8

3 3-NOR

4013

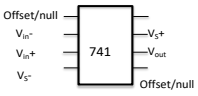
1 (Q)		(V+)	14
2 (!Q)		(Q)	13
3 (C)		(!Q)	12
4 (R)		(C)	11
5 (D)		(R)	11
6 (S)		(D)	10
7 (Gnd)		(S)	9

Dual D-FF

4017

1 (5)		(V+)	16
2 (1)		(R)	15
3 (0)		(CLK)	14
4 (2)		(CKE)	13
5 (6)		(CO)	12
6 (7)		(9)	11
7 (3)		(4)	10
8 (Gnd)		(8)	9

Counter

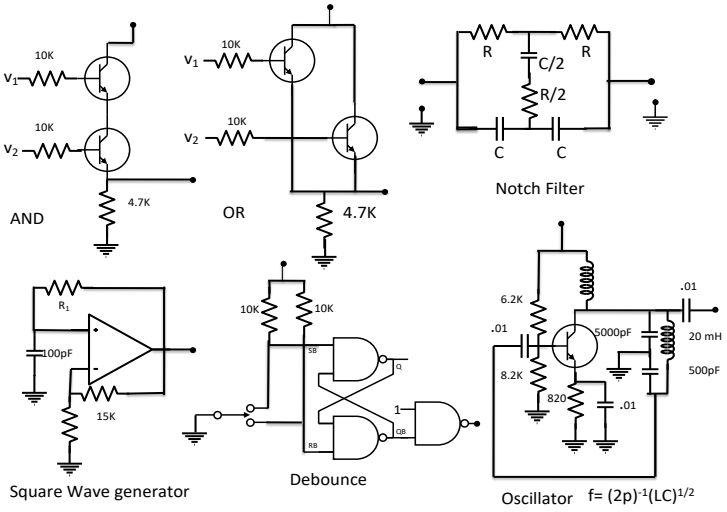


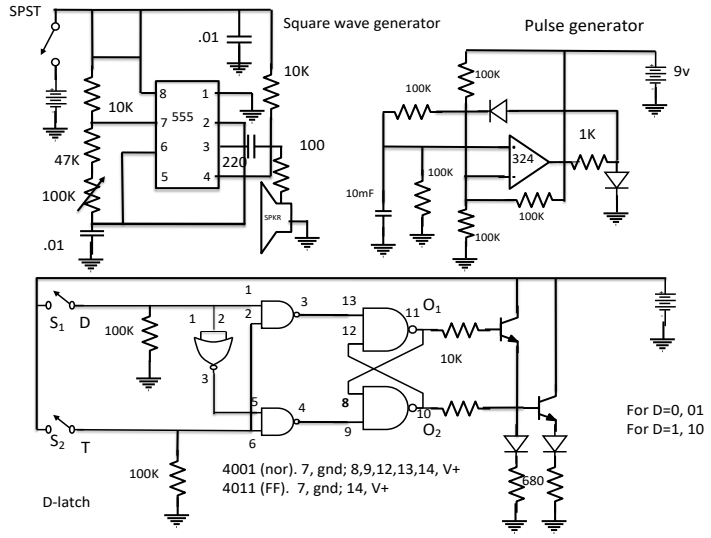
1 (o1)		(o4)	14
2 (i1-)		(i4-)	13
3 (i1+)		(i4+)	12
4 (V+)		(GND)	11
5 (i2+)		(i3-)	10
6 (i2-)		(i3+)	9
7 (o2)		(o3)	8

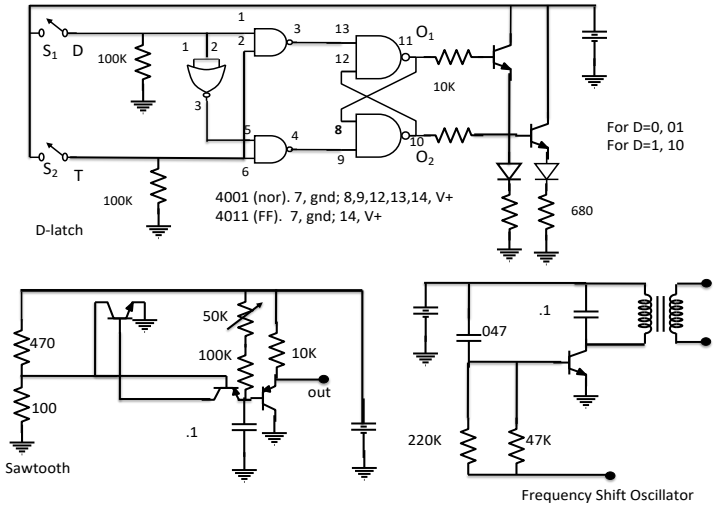
324 op amp

1 (GAIN)		(GAIN)	8
2 (IN-)		(BYP)	7
3 (IN+)		(V+)	6
4 (GND)		(OUT)	5

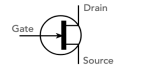
386 amp


10K
V1
10K
V2
4.7K
AND
OR
4.7K
R
C/2
R
R/2
C
C
Notch Filter
R1
100pF
15K
Square Wave generator
10K
10K
SB
RB
Q
QB
Debounce
6.2K
.01
.01
5000pF
20 mH
500pF
8.2K
820
.01
Oscillator f= (2p)-1(LC)1/2


SPST
Square wave generator
.01
10K
10K
8
1
7
555
2
6
3
5
4
47K
100K
220
100
SPKR
.01
Pulse generator
9v
100K
100K
1K
324
10mF
100K
100K
100K
S1
D
100K
1
2
3
13
11
O1
12
10K
S2
T
100K
D-latch
4001 (nor). 7, gnd; 8,9,12,13,14, V+
4011 (FF). 7, gnd; 14, V+
8
10
O2
680
For D=0, 01
For D=1, 10



FETs



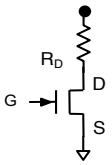
N channel JFET

From electronics notes

N channel enhancement insulated MOSFET

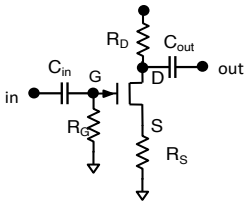
source gate drain
2N-7000 package

- Small signal model
- $i_D = i_{DSS}(1 - \frac{V_{GS}}{V_p})^2, 0 \le V_{GS} \le V_P$
- Ohmic ($V_{DS} < 1.8$), $R_{GS} = \frac{k}{g_m} V_{GS}$.
- Saturation ($V_{DS} > 2$), $i_d = g_m V_{GS}$
- For 2N-7000, $I_{DSS} = 60, g_m = 320$



- JFETs generally don't operate in enhancement mode ($V_{GS} < 0$)

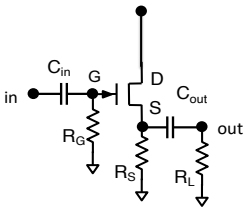
FETAmps

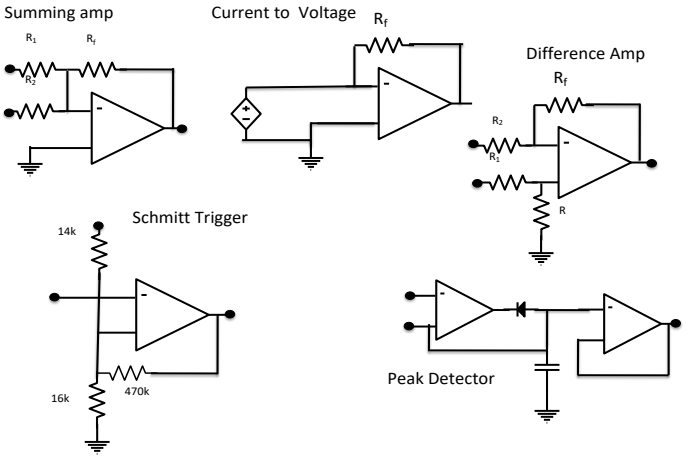


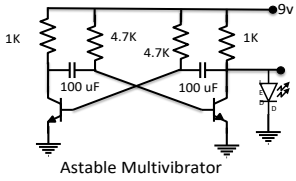
- Common Source

1. $V_{DD} = 12v, i_{DSS} = 35mA, V_p = -3v$
2. $A_V = 10, i_{DQ} = 10mA$
3. $R_S = -\frac{V_P}{i_{DQ}}(1 - \sqrt{\frac{i_{DQ}}{i_{DSS}}})$= 139 (say 150Ω)
4. $A_V = -\frac{R_D}{R_S}$, $R_D = 1{,}500\Omega$

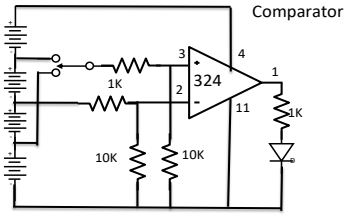
- Common Drain



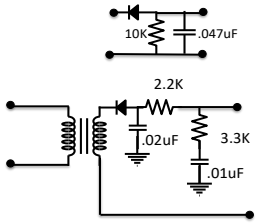




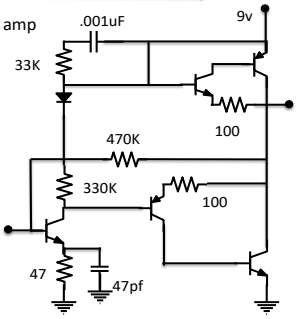
Astable Multivibrator



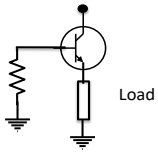
AM Detectors

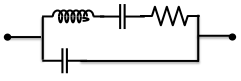


Push-pull amp



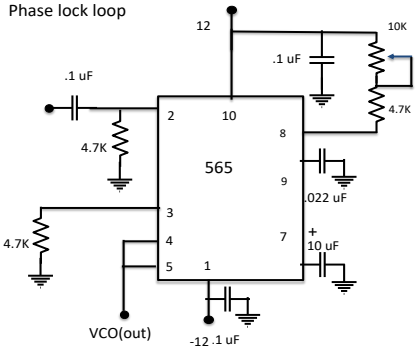
Current source



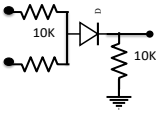


Crystal equivalent

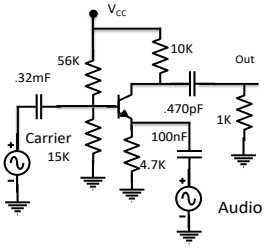
Phase lock loop

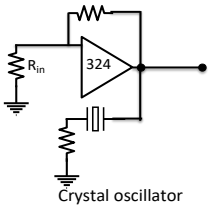


Mixer



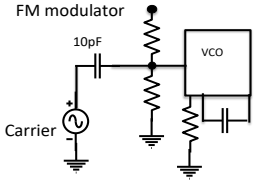
AM modulator

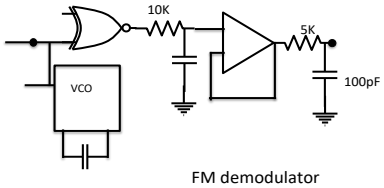




Crystal oscillator

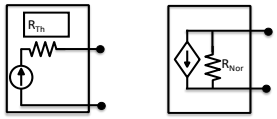
FM modulator





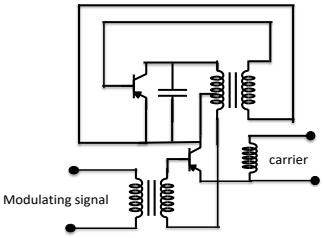
FM demodulator

Thevenin, Norton and two port models

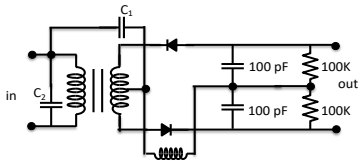


- Two port model
- $\begin{pmatrix} i_1 \\ i_2 \end{pmatrix} = \begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{bmatrix} \begin{pmatrix} V_1 \\ V_2 \end{pmatrix}$

FM Ratio Modulator



FM Ratio Detector



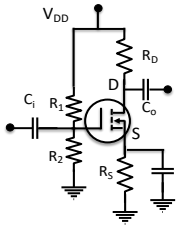
$$f_c = \frac{1}{2\pi\sqrt{L_1 C_2}}$$

L_1 is the transformer input inductance

C_1 is a DC block

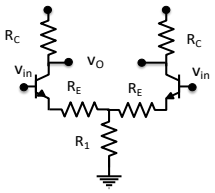
CMOS Common Emitter amp

- Pick power
- $V_{DD} = i_D R_D + V_{DS} + i_D R_S$
- $V_{GS} = V_G - i_S R_S$
- $V_G = V_{DD} \frac{R_1}{R_1 + R_2}$
- $i_D = k(V_G - V_{TH})^2$
- Bias around $\frac{V_{DD}}{3}$
- Pick gain, $A = \frac{R_D}{R_S + \frac{1}{gm}}$



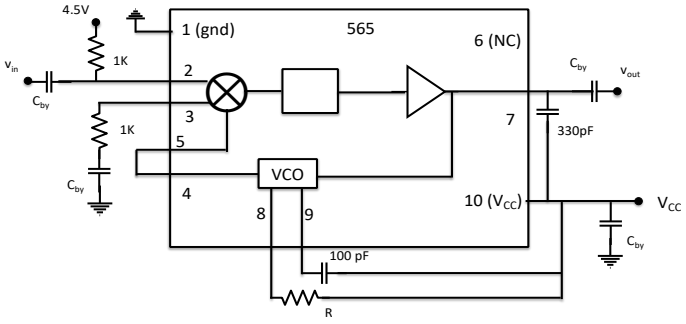
- Two port model
- $\begin{pmatrix} i_1 \\ i_2 \end{pmatrix} = \begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{bmatrix} \begin{pmatrix} V_1 \\ V_2 \end{pmatrix}$

Differential amp

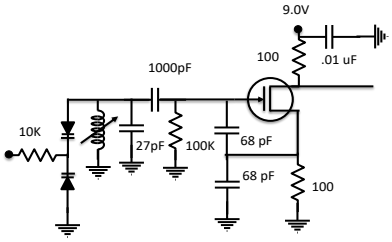


- Pick power ∓ 12
- Choose collecter current ($2mA$) by picking R_1
- Pick gain, $A = \frac{R_C}{2R_E}$

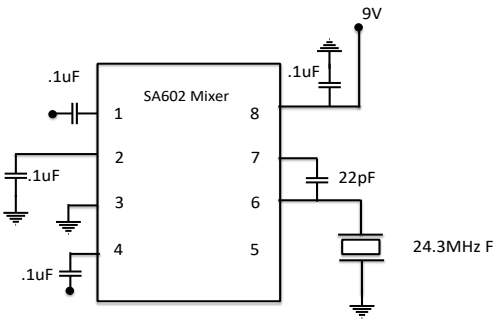
PLL as FM detector with 565

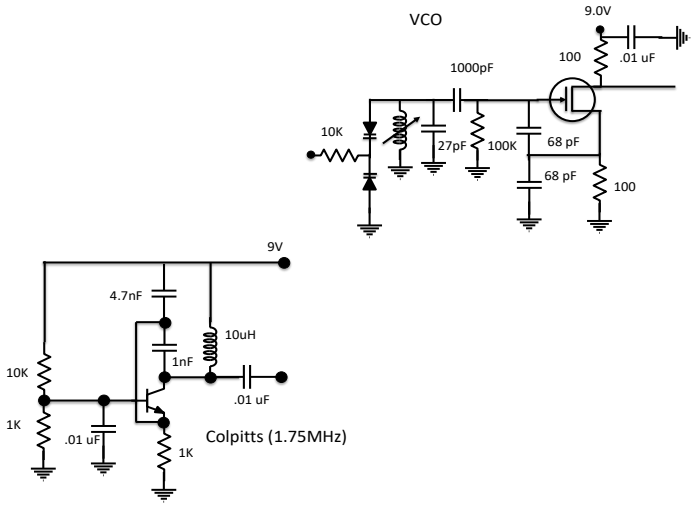


VCO

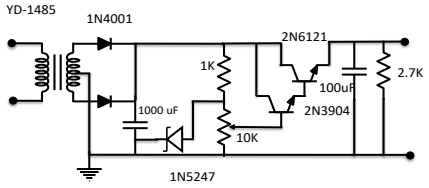

9.0V
100
.01 uF
1000pF
10K
27pF
100K
68 pF
68 pF
100

SA612

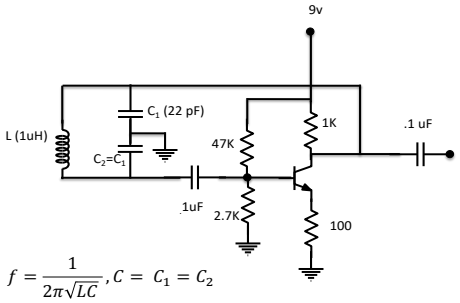

9V
.1uF
.1uF
SA602 Mixer
1
2
3
4
8
7
6
5
.1uF
22pF
.1uF
24.3MHz F



Variable power supply



Colpitts



$f = \frac{1}{2\pi\sqrt{LC}}, C = C_1 = C_2$
About 32MHz in this example
About 23MHz if C= 47pF

Real components: *Real amp:* $A = \frac{I_C R_C}{\frac{kT}{q}}$ and $I_C = \frac{V_{BB}-V_{BE}}{R_E}$, $i_c \approx \frac{v_{BB}-v_{BE}}{R_E}, v_{BB} = v_{CC}\frac{R_{B2}}{R_{B1}+R_{B2}}$, frequency response is $\frac{1+j\omega C_1 R_2}{\sqrt{1+\omega^2(r_1^2C_1^2+R_2^2C_2^2)+\omega^4(R_1C_1R_2C_2)^2}}$.
Air coil (solenoid): $L = \frac{\mu n^2 A}{l}$.
Air coil: $L(\mu H) = \frac{d^2n^2}{18d+40l}$ (length in inches).
Torodal coil, powdered iron: $L(\mu H) = \frac{A_L n^2}{10^3}$ (length in inches).
Torodal coil, ferrite: $L(\mu H) = \frac{A_L n^2}{10^6}$ (length in inches).
Wire gauge diameter: 22 - 25 mil, 20 - 32 mil, 12 - 80 mil. 1 mil= .0254 mm.

Fourier representation: $V(t) = \frac{a_0}{2} + \sum_{n=1}^{\infty}(a_n cos(n\omega t) + b_n cos(n\omega t))$, $a_n = \int_{T/2}^{T/2} V(t)cos(n\omega t)$, $b_n = \int_{T/2}^{T/2} V(t)sin(n\omega t)$.

Reflection on string: $\frac{\partial^2\psi}{\partial t^2} = \frac{T}{\rho}\frac{\partial^2\psi}{\partial x^2}$, $v_\phi = \frac{\omega}{k}$, $v_g = \frac{d\omega}{dk}$, $Z = \sqrt{T\rho}$. *Power:* $P(t) = F\frac{\partial\psi}{\partial t}$, For travelling wave: $P(t) = Z(\frac{\partial\psi}{\partial t})^2$. Consider a wave train on a string from the left (L) with a change at $x = 0$ of medium (i.e. a denser string) to a string on the right (R). Dispersion caused by variation of wave velocity by frequency relation $\omega = f(k)$. Consider string of density μ_1 connected to string of density μ_2 at 0. $f_1(x - \frac{x}{v_1}) + g(x + \frac{x}{v_1}) = f_2(x - \frac{x}{v_2})$. At 0: $f_1(t) + g(t) = f_2(t)$ and $\frac{f_1'(t)}{v_1} - \frac{g'(t)}{v_1} = \frac{f_2'(t)}{v_2}$; solve to get $g(t) = \frac{v_2-v_1}{v_2+v_1}f_1(t)$ and $f_2(t) = \frac{2v_2}{v_2+v_1}f_1(t)$. *Mach angle:* $sin(\theta) = \frac{u}{v}$. For perfect termination: $F_{term}(\text{“R on L”}) = -Z_L\frac{\partial\psi_{inc}}{\partial t}(0,t)$. For excess force: $F_{term}(\text{“R on L”}) = Z_L\frac{\partial\psi_{ref}}{\partial t}(0,t)$. $-Z_L\frac{\partial\psi_{inc}}{\partial t}(0,t) + Z_L\frac{\partial\psi_{ref}}{\partial t}(0,t) = -Z_R(\frac{\partial\psi_{inc}}{\partial t}(0,t) + \frac{\partial\psi_{ref}}{\partial t}(0,t))$. So, $\frac{\partial\psi_{ref}}{\partial t}(0,t) = \frac{Z_L-Z_R}{Z_L+Z_R}\frac{\partial\psi_{inc}}{\partial t}(0,t)$. $R = \frac{Z_L-Z_R}{Z_L+Z_R}$ is called the reflection coefficient.

Transmission boundary: Let $v_I(\frac{x}{v_1} - t), x < 0$, $v_R(\frac{x}{v_1} + t), x < 0$, $v_T(\frac{x}{v_2} - t), x > 0$ be respectively the incidence, reflection and transmission voltages of a transmission line with boundary at $x = 0$. Put $x = 0$

to get $v_I(t) + v_R(t) = v_T(t)$. Expressing the current flow at the boundary in terms of the voltages and the impedences ($Z_L, x < 0$ and $Z_R, x > 0$), we get $\frac{v_I(t)}{Z_L} - \frac{v_R(t)}{Z_L} = \frac{v_T(t)}{Z_R}$. Solving we get, $v_R(t) = \frac{Z_L - Z_R}{Z_L + Z_R} v_I(t)$ and $v_T(t) = \frac{2Z_R}{Z_L + Z_R} v_I(t)$.

Wave Transmission: *String:* $v = \sqrt{\frac{F}{\mu}}$. *Fluid:* $v = \sqrt{\frac{B}{\rho}}$. *Solid:* $v = \sqrt{\frac{Y}{\rho}}$. *Adiabatic Gas:* $v = \sqrt{\frac{\gamma p}{\rho}}$.
Diffraction: $I = I_0(\frac{sin(\frac{\beta}{2})}{\frac{\beta}{2}})^2$, $\beta = \frac{2\pi a sin(\theta)}{\lambda}$.
Standing wave transmits no energy.

Early Quantum Mechanics: $\Delta p \Delta x \geq \frac{h}{4\pi}$, $\hbar = \frac{h}{2\pi}$, $\lambda = \frac{h}{p}$, $\nu = \frac{E}{h}$, $p = \frac{hk}{2\pi} = \frac{p}{\lambda}$, $E = \frac{h\omega}{2\pi}$, $p_{av} = nkT$. *Blackbody radiation:* $E(\lambda, T) = \frac{8\pi hc}{(\lambda^5)}(e^{(hc)/(\lambda kT)} - 1)^{-1}$. *Photoelectric Effect:* $hf = KE + \phi$. *Bohr hydrogen atom:* $E_n = -\frac{13.6ev}{n^2}$, $r_n = n^2 a_0$, $a_0 = \frac{h^2}{2\pi kmc^2} = .0529nm$. *Time Independent Schrodinger:* $\frac{d^2\psi}{dt^2} + \frac{4\pi m}{h}(E - U(x))\psi = 0$. *Schrodinger:* $\frac{ih}{2\pi}\frac{\partial \psi}{\partial t} = -\frac{h^2}{8\pi^2 m}\nabla^2\psi + V\psi$.

General Relativity: The *proper interval* is $I(x, y, z, t) = c^2t^2 - (x^2 + y^2 + z^2)$, $I(x, y, z, t) = I(x', y', z', t')$. $ds^2 = g_{ij}dx^i dx^j$, $g_{ij} = g_{ji}$, $\delta \int ds = 0$. The *action* is $S = \int_{t_1}^{t_2} L(x, x', t)dt$, $\delta S = 0 \rightarrow \frac{\partial L}{\partial x} - \frac{d}{dt}\frac{\partial L}{\partial x'} = 0$. $L(x, x', t) = \frac{-m_0 c^2}{\sqrt{1 - \frac{v^2}{c^2}}} - q(\phi + v \cdot A)$. $R_{excess} = \sqrt{\frac{A}{4\pi}} - r_{meas} = \frac{G}{3c^2}M$, $\frac{G}{3c^2} = 2.5 \times 10^{-29}\frac{cm}{gm}$. From principle of equivalence, $\omega = \omega_0(1 + \frac{gH}{c^2})$ - doppler shift measured by Pound and Rebka. $\tau = \frac{L}{c}$ and $L = \int_0^t ||\dot{X}(t)||dt$. *Equation of motion:* $\frac{d^2X}{d\tau^2} = -\Gamma^i{}_{kl}\frac{dX^k}{d\tau}\frac{dX^l}{d\tau}$; this corresponds to Newtonian $\ddot{x}^\alpha = -\frac{\partial \Phi}{\partial x^\alpha}$.

Maxwell's equations (CGS): $\nabla \cdot \vec{j} = -\frac{\partial \rho}{\partial t}$, $\nabla \cdot \vec{E} = 4\pi\rho$, $\nabla \times \vec{E} = -\frac{1}{c}\frac{\partial \vec{B}}{\partial t}$, $\nabla \cdot \vec{B} = 0$, $\nabla \times \vec{B} = \frac{4\pi}{c}\vec{j} + \frac{1}{c}\frac{\partial \vec{E}}{\partial t}$.

CGS Units: $k = 1$. $F = q(E + \frac{v}{c} \times B)$. 1 statvolt= 300 volts
1 statvolt/cm = 3×10^4 volts/m
1 T = 10^4 G
1 C = 3×10^9 esu
1 ohm = 1.139×10^{-12} sec/cm
1 weber = 10^8 G-cm
1 J = 10^7 ergs
1 N = 10^5 dynes

4.2 Physical Constants

Conversion factors: 1 $in = 2.54$ cm. 1 $meter = 39.370$ in. 1 $AU = 1.496 \times 10^{11}$ m. 1 $lb = 4.448$ N. 1 $Pa = 1$ $\frac{N}{m^2}$. 1 $Atm = 1.013 \times 10^5$ Pa. 1 $hp = 745.7$ W. 1 $J = 10^7$ erg. 1 $ev = 1.602 \times 10^{-19}$ J. 1 $BTU = 1055$ J. 1 $cal = 4.186$ J. 1 $L = 1000$ cm^3. 1 $Gal = 3.785 \times 10^{-3}$ m^3. 1 $kg = 2.2046$ lbs, 1 $fluid - oz = 0.0338$ ml, 1 $gal = 3.3785$ $liters$.

Atomic constants: $M_e = .510998$Mev $= 9.10939 \times 10^{-31}kg$, $M_p = 938.256$Mev$(= 1836M_e) = 1.67262 \times 10^{-27}kg$, $M_n = 939.55$Mev $= 1.67493 \times 10^{-27}kg$, $\sigma_{SB} = 5.67 \times 10^{-8}Wm^{-2}K^{-4}$, $1ev = 1.6 \times 10^{-12}erg = 1.6 \times 10^{-19}J$, $1curie = 3.7 \times 10^{12}decays$, $c_s = 3.32 \times 10^4 cm/s$, $1kgTNT = 4.2MJ$, $1A = 10^{-8}cm$. *HDNA:* 2,900,000 kilobases.

System	ϵ_0	μ_0	$\vec{D}, \vec{H}$	Maxwell's equations	Lorentz Force
Gaussian	1	1	$\vec{D} = \vec{E} + 4\pi\vec{P}$ $\vec{H} = \vec{B} - 4\pi\vec{M}$	$\nabla \cdot \vec{D} = 4\pi\rho$ $\nabla \times \vec{H} = \frac{4\pi\vec{j}}{c} + \frac{1}{c}\frac{\partial\vec{D}}{\partial t}$ $\nabla \cdot \vec{B} = 0$ $\nabla \times \vec{E} + \frac{1}{c}\frac{\partial\vec{B}}{\partial t} = 0$	$q(\vec{E} + \frac{\vec{v}}{c} \times \vec{B})$
MKS	$\frac{10^{-9}}{36\pi}$	$4\pi \times 10^{-7}$	$\vec{D} = \epsilon_0\vec{E} + \vec{P}$ $\vec{H} = \frac{\vec{B}}{\mu_0} - \vec{M}$	$\nabla \cdot \vec{D} = \rho$ $\nabla \times \vec{H} = \vec{j} + \frac{\partial\vec{D}}{\partial t}$ $\nabla \cdot \vec{B} = 0$ $\nabla \times \vec{E} + \frac{\partial\vec{B}}{\partial t} = 0$	$q(\vec{E} + \vec{v} \times \vec{B})$

Figure 4.1: Maxwell's Equations in MKS and CGS

Astronomical constants: $H_0 = 100$km(s-Mpc)$^{-1}$, 1 pc $= 3.26l-y$, 10^{80}nucleons, 10^{28}cm-diam, 10^{11}galaxies.
Milky Way: $\epsilon_{ecliptic/MW} = 62.5$, 1.6×10^{11}stars, 10^{23}cm-diam, 8×10^{44}gm.
Sun: $E_{sun} = 4 \times 10^{33}$ergs/sec, $R_{Sun} = 3.5 \times 10^{10}cm$, 1.99×10^{33}gm, $\lambda_{sun} = 30days$.
Earth: $\epsilon_{earth} = 23.5$, 50% clouds, $R_{moon} = 2160mi$, $\epsilon_{moon} = 5$, $\lambda_{sider} = 27d7h43m12s$, $\lambda_{synod} = 29d12h44m3s$, $D_{moon} = 363,300 - 405,500km$. $RA_{Greenwich}(1986.0) : 6.6245$, 0 Jan 1986 $= 2,446,430.5JD$.

Geological: For seismic wave, $v_P = \sqrt{\frac{(k+\frac{4}{3}\mu)}{\rho}}$, $v_S = \sqrt{\frac{\mu}{\rho}}$.
$\mu_{granite} = 1.6 \times 10^{10} dynes/cm$, $k_{granite} = 27 \times 10^{10} dynes/cm$, $k_{water} = 2.0 \times 10^{10} dynes/cm$, $\mu_{water} = 0$.
$v_{P-granite} = 5.5km/sec$, $v_{S-granite} = 3.0km/sec$, $v_{P-water} = 1.5km/sec$, $v_{S-water} = 0$.

Materials: *Young's Modulus:* $\frac{F}{A} = Y\frac{\Delta L}{L}$.
Bulk Modulus: $\frac{F}{A} = B\frac{\Delta V}{V}$.
Shear Modulus: $\frac{F}{A} = G\frac{\Delta x}{L}$.
Viscosity: $\eta = \frac{\frac{F}{A}}{\frac{\Delta v}{h}}$.
Surface tension: $\gamma_{H_2O} = 72.8 \times 10^{-4} N/m$.
Reynold's number: $Re = \frac{\rho\bar{v}L}{\eta}$; turbulent flow if $Re > 4000$, laminar if $Re < 2000$.
Dry (static, sliding) Friction: Steel (.78,.42), Teflon; (.04,-).
Expansion: $\alpha_l = l^{-1}\frac{\partial l}{\partial t} \times 10^6$, C: (Al, 24), (Cu, 17), (Granite, 8.3), (Ice, 50), (Fe, 12), (Water, 207).
Heat Capacity: $c_v = m^{-1}\frac{\partial Q}{\partial T} : [\frac{J}{mol-^oK}]$ (He, 12.5), (O_2, 21.1), (N_2, 20.6), (C_2H_6 , 39.3), MFP $N_2 = 10^{-5}$ cm, $C_{v,solid} = 3R$.
$c_{v,air} \approx 700\frac{J}{kg-^oK}$. *Melting/Boiling:* MP/BP (K): Au, 1336, 3081; O_2, 54, 90; Cu, 1356, 2839.
Heat Conduction: $Q' = -\kappa A\frac{\partial T}{\partial l}W(cmK)^{-1}$: (Cu, 4), (Fe, 0.80), (Si, 1.5), (H_2,.00024-.0018), (Rock, 2.8 kc/mhK).
Dielectric: $\epsilon = K\epsilon_0$: (Glass, 6.7), (Water, 78), (Nylon, 3.6).
Resistivity: $R = \rho\frac{L}{A} \times 10^{-8}$: (Ag, 1.4), (Cu, 1.7), (Al, 2.8), (Fe, 9.8).
Density: ρ/ρ_{water}: Al, 2.7; Cu, 8.9; Rock, 5.5; Au, 19; Fe, 7.8; Gas, .68 (g/cm^3); air, .0012; wood, .75.
Moduli: $B = \frac{\frac{\Delta P}{A}}{\frac{\Delta V}{V}}$: Al, 70; Cu, 140; Fe, 100; Water, 2.2 (GPa).
$Y = \frac{\frac{\Delta F}{A}}{\frac{\Delta l}{l}} \times 10^{12} dy/cm^2$: Al, 70; Cu, 110; Fe, 190.
$M_s = \frac{\frac{\Delta F}{A}}{\frac{\Delta x}{l}}$: Al, 30; Cu, 42; Fe, 100.

Energy content of one gallon of heating oil: $140,000kJ/gallon$.

Air: 28.96 m-w, c_p = 1005 J/kg-K, $c_v = 718J/kg - K$. $1\ atm = 1.013 \times 10^5 Pa$, $Pa = 10^6 dyne/cm^2 = 1N/m^2 = 760mm - Hg$. $\rho : 1.293mg/cm^3$, $\kappa : 2.4 \times 10^{-2} W/m - K$, $visc@20 : .00018g/cm - s$.

Water: 273.15K, 18 m-w, 540 cal/gm (vaporization), 80 cal/gm (fusion), $\rho_{ice} = 917kg/m^3$, $\rho_{water} = 1g/cm^3$, $\kappa : .19W/m - K, visc@20 : .01gm/cm - s, ST : @20 : 73d/cm$. Specific heat of water: $1cal/K - gm = 4.186J/K - gm$.

Sound: *Sound strength:* $g = 10log(\frac{I}{I_0})$ in db. $I_0 = 10^{-12} W/m^2$. Normal Conversation: 60 db, Jet: 130 db. *Speed of Sound:* $\approx 330m/s$ at normal conditions, $v_{av} = \sqrt{3kT/m}$.

Name	**RA**	**Dec**	**Vmag**	**Dist**	**Name**	**RA**	**Dec**	**Vmag**	**Dist**
Polaris	01 23	88 46	2.06	200	Mizar	13 20	55 27	2.12	26
Aldeberan	04 30	16 19	.8	21	Capella	05 09	45 54	.09	14
Rigel	05 10	-08 19	.11	270	Bellatrix	05 20	06 16	1.63	140
Betelgeuse	05 50	07 23	.4	180	Sirius	06 41	-16 35	-1.44	2.7
Canopus	06 22	-52 38	-.72	?	Castor	07 28	32 06	1.56	14
Procyon	07 34	05 29	.36	3.5	Pollux	07 39	28 16	1.15	10.7
Regulus	10 03	12 27	1.34	26	Merak	10 56	56 55	2.36	23
Spica	13 20	-10 38	.97	65	Arcturus	14 11	19 42	-.05	11
Antares	16 23	-26 13	.94	130	Vega	18 34	38 41	.03	8.1
Altair	19 46	08 36	.77	4.9	Deneb	20 38	44 55	1.25	500

Figure 4.2: Stars

Planet	$\mathbf{D_{av}(km \times 10^6)}$	λ**(rev)**	**e**	**i**	$\mathbf{L_{node}}$	$\mathbf{L_{Per}}$	$\mathbf{P_{epoch}}$	**M(gm)**	**R(km)**	**Rot**
Mercury	57.9	87.97d	.2	7	47.9	76.8	222.6	3.3e26	2439	58.7d
Venus	108.2	224.7d	.007	3.4	76.3	131.0	174.3	4.9e27	6050	243d
Earth	149.6	365.26	.017	0	0	102.3	100.2	6e27	6378	23h56m
Mars	227.9	686.98	.093	1.8	49.2	335.3	258.8	6.4e26	3394	24h37m
Jupiter	778.3	11.8yr	.048	1.3	100.0	13,7	259.8	1.9e30	71880	9.8h
Saturn	1427.0	29.46	.056	2.5	113.3	92.3	280.7	5.7e29	60400	10.66h
Uranus	2869	84	.047	.8	73.8	170.0	141.3	8.8e28	23540	17.24h
Neptune	4496	164.79	.009	1.8	131.3	44.3	216.9	1e29	24600	16h
Pluto	5900	247.7	.250	17.2	109.9	224.2	181.6	-	-	-

Figure 4.3: Planetary data - Epoch: 1960 Jan 1.5UT, Orbit: $a = b\sqrt{1 - e^2}$.

Stellar Evolution ($'$: means differentiate wrt r): $P' = -\rho \frac{GM(r)}{r^2}$, $M' = 4\pi r^2 \rho$, $L' = 4\pi r^2 \epsilon$, $L' = \frac{(-3\chi\rho)}{(4acT^3(4\pi r^2))}$ (rad), $L' = (1 - \gamma^{-1}) T \rho^{-1} P'$ (conv), $P = RT\frac{\rho}{\mu}$, $\chi = C\rho T^{-3.5}$, $\alpha = \frac{10^6}{T^{1/3}}$.

Place	Lat	Long	Place	Lat	Long	Place	Lat	Long
Beijing	40.1	116.33	SF	37.45	-122.33	NY	41.44	-73.8
Boston	42.35	-71.05	Chicago	41.87	-87.63	Dallas	32.78	-96.78
Madison, Wi	43.07	-89.38	Santa Fe	35.68	-105.93	Seattle	47.61	-122.33
Tucson	32.22	-110.97	DC	38.88	-77.0	Denver	39.75	-104.99
Atlanta	33.75	-84.39	London	51.5	0.0	Paris	48.83	2.3
Berlin	52.5	13.42	Rome	41.88	12.5	Moscow	55.75	37.7
Athens	37.97	23.75	Jerusalem	31.75	35.22	Tokyo	35.75	139.75
Sidney	-33.87	151.2	MKea	19.826	-155.47	CTlo	-70.82	-30.17
New Orleans	29.93	-90.07	Redmond,OR	44.27	-121.15	Portland	45.52	-122.68
LA, CA	34.05	-118.24	San Diego	32.7	-117.15	Orlando	28.52	-81.38
Milan	45.45	9.28	Amsterdam	52.3	4.77	Auckland	-36.92	138.58
Bombay	18.93	74.58	Delhi	28.67	77.23	Perth	-31.93	-115.83
Toronto	43.65	-79.38	Bagdad	33.3	44.43	Cairo	30.03	31.35

Figure 4.4: Places on Earth

Optics: $n_{glass} = 1.52$, $n_{water} = 1.33$, $n_{diamond} = 2.42$. *Lensmaker's law (air to glass, one surface):* $\frac{1}{s} + \frac{n}{s'} = \frac{1}{f}$. *Lensmaker's law (double surface):* $\frac{n_1}{s} + \frac{n_2}{s'} = \frac{1}{f}$, $\frac{1}{f} = (n_2 - n_1)\frac{1}{R_1} - \frac{1}{R_2}$. $\frac{h_i}{h_o} = \frac{d_i}{f} = \frac{f}{d_o}$. *Resolving Power:* $4.54/D_{inches}$ arc-seconds, $f_{ratio} = \frac{L_{focus}}{R_{diameter}}$, $3 \leq f_{ratio} \leq 6$, $Mag = \frac{L_{focus-objective}}{L_{focus-eyepiece}}$. *Lens:* Original object PA of height y with ray intersecting focus at S hitting lens at U to (inverted) image BR of height y'. Similarly, ray from P parallel to axis hitting lens at Q intersecting focus at T. x is distance from A to S and x' from T to B; finally, f is the distance from the focus to the lens. $\frac{PA}{AS} = \frac{QU}{PQ}$ and $\frac{BR}{TB} = \frac{QU}{UR}$. Thus, $\frac{y}{x} = \frac{y+y'}{x+f}$ and $\frac{y'}{x'} = \frac{y+y'}{x'+f}$. $f^2 = xx'$. *Magnification:* $\frac{y}{y'} = \frac{x'}{f} = \frac{f}{x}$.

Chemical bonds: *Covalent:* 80-200 kcal/mole (C=C is 200), *Ionic:* 4-7 kcal/mole, *Hydrogen:* 5kcal/mole, *VanderWaal:* $< 1kcal/mole$ (methane). *Thermal:* .6 kcal/mole. Acid added to H_2O increases $H^+, pH = -log[H^+]$, acid < 7.

Fluids: $P + \phi + \frac{1}{2}\rho v^2 = const$, $\nabla \rho v = -\rho'$, $\nabla v = 0$, $\nabla \times v = 0$.

Interference: $R = A[cos(\omega t) + cos(\omega t + \phi) + \ldots + cos(\omega t + (n-1)\phi)]$. $A_R = A\frac{sin(\frac{n\phi}{2})}{sin(\frac{\phi}{2})}$. $I = I_0\frac{sin^2(\frac{n\phi}{2})}{sin^2(\frac{\phi}{2})}$. For $f(t) = A_1 e^{i\omega_1 t} + A_2 e^{i\omega_2 t}$, $I = A_1^2 + A_2^2 + 2cos((\omega_1 - \omega_2)t)$. Group velocity and modulation.

Damped and driven simple harmonic oscillators: Solution of $m\ddot{x} + kx = 0$ is $Acos(\omega t) + Bsin(\omega t)$ where $\omega = \sqrt{\frac{k}{m}}$. Solution of $m\ddot{x} + b\dot{x} + kx = 0$ is $e^{-\omega_0 t}(Acos(\omega t) + Bsin(\omega t))$ where $\omega = \frac{\sqrt{b^2 - 4km}}{2m}$ and $\omega_0 = \frac{b}{2m}$. Solution of $m\ddot{x} + b\dot{x} + kx = Fcos(\gamma t)$ is $e^{-\omega_0 t}(Acos(\omega t) + Bsin(\omega t)) + \alpha cos(\gamma t) + \beta sin(\gamma t)$ where $\alpha = F\frac{k - m\gamma^2}{(b\gamma)^2 + (k - m\gamma^2)^2}$ and $\beta = F\frac{b\gamma}{(b\gamma)^2 + (k - m\gamma^2)^2}$.

Spectrum: 30cps audio 30K 500K AM 1500K 3M HF 30M 88M FM VHF 210M 400M UHF 800M 1.5G H_2 S-band 3G 7600A IR 6300 Visible 3900A UV 100A X-ray .1A gamma 67 Mev.
IEEE: HF ($.003 - .03$ G), VHF ($.03 - .3$ G), UHF ($.3 - 1$ G), L ($1 - 2$ G), S ($2 - .4$ G), C ($4 - 8$ G), X ($8 - 12$ G), Ku ($12 - 18$ G), K ($18 - .27$ G), Ka ($27 - 40$ G), V ($40 - 75$ G), W ($75 - 110$ G), G ($110 - 300$ G). Red: 650nm, Yellow: 580 nm, Green: 500nm, Blue: 475nm, Violet: 400Nm.

Fris and dB: dBm- relative to 1 mW, dBc - relative to carrier. $P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2}$. 120 dB at 433MHz, $d = 2km$.

Radar range equation: $R^4 = \frac{P_{tx} G^2 \sigma \lambda^2}{(4\pi)^3 P_{rx,min)}}$, $P_{rx,min} = kTBF(SNR)_{min}$.

Middle C: 256Hz. Octave has 12 notes in uniformly divided log scale. Octave is factor of 2.

Central Forces: $\vec{a}(r) = f(r)\hat{r}$. $(\ddot{r} - r\dot{\theta}^2) = f(r)$ and (conservation of angular momentum), $(r\ddot{\theta} + 2\dot{r}\dot{\theta}) = 0$. $r^2\dot{\theta} = h$. $u = \frac{1}{r}$ implies $\frac{d^2u}{d\theta^2} + u = \frac{k}{h^2}$, $k = GM$, h is angular momentum. Then $r = \frac{h^2}{k(1+ecos(\theta))}$. If $V(r) = -\int f(r)dr$, $\frac{1}{2}m(\dot{r}^2 + r^2\dot{\theta}^2) + V(r) = E$; ellipse if $E < 0$, parabola if $E = 0$, hyperbola if $E > 0$.

Rotating frames: Suppose $XYZ(F)$ is inertial system and $xyz(M)$ is rotating frame with a common origin O. $(\frac{d\vec{A}}{dt})_{|F} = (\frac{dA}{dt})_{|M} + \omega \times \vec{A}$. ${D_F}^2\vec{r} = {D_M}^2\vec{r} + D_M(\vec{\omega}) \times \vec{r} + 2\vec{\omega} \times D_M\vec{r} + \vec{\omega} \times (\vec{\omega} \times \vec{r})$. Last two terms are coriolis and centripetal. If O is moving too, $D_F(\vec{r}) = \dot{R} + D_M\vec{r} + \vec{\omega} \times \vec{r}$ and ${D_F}^2\vec{r} = \ddot{R} + {D_M}^2\vec{r} + D_M(\vec{\omega}) \times \vec{r} + 2\vec{\omega} \times D_M\vec{r} + \vec{\omega} \times (\vec{\omega} \times \vec{r})$. Object dropped from rotating sphere from a height h is deflected by $\frac{1}{3}\omega g t^3 sin(\lambda)$, where λ is the colatitude.

Foucault (constrained to horizontal plane): $m\ddot{x} = -T(\frac{x}{l}) + 2m\omega\dot{y}cos(\lambda)$, $m\ddot{y} = -T(\frac{y}{l}) - 2m\omega(\dot{x}cos(\lambda) - \dot{z}sin(\lambda))$, $m\ddot{z} = -T(\frac{l-z}{l}) - mg + 2m\omega\dot{y}sin(\lambda)$, $\hat{n} = isin(\omega cos(\lambda)t) + jcos(\omega cos(\lambda)t)$.

Navigation and accelerometers: Roll is $R_x(\phi) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & cos(\phi) & -sin(\phi) \\ 0 & sin(\phi) & cos(\phi) \end{pmatrix}$.
Pitch is $R_y(\theta) = \begin{pmatrix} cos(\theta) & 0 & -sin(\theta) \\ 0 & 1 & 0 \\ sin(\theta) & 0 & cos(\theta) \end{pmatrix}$. Yaw is $R_z(\psi) = \begin{pmatrix} cos(\psi) & -sin(\psi) & 0 \\ sin(\psi) & cos(\psi) & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Earth orientation to body orientation is done by $R_{xyz} = R_x(\phi)R_y(\theta)R_z(\psi)$. So accelerometer reading is $G_p = R_{xyz}(0,0,1)^T$ and $h = \frac{G_p}{||G_p||} = \begin{pmatrix} -sin(\theta) \\ cos(\theta)sin(\psi) \\ cos(\theta)cos(\psi) \end{pmatrix}$. For tilt orientation, $tan(\psi_{xyz}) = \frac{h_y}{h_z}$. $tan(\theta_{xyz}) = \frac{-h_x}{\sqrt{{h_y}^2 + h_z^2}}$.

Rotation in plane: $I = \int r^2 dm$. $\vec{\Omega} = I\vec{\omega}$, $T = \frac{1}{2}I\omega^2$ $\vec{\Lambda} = I\dot{\vec{\omega}}$. *Parallel axis theorem:* $I_A = I_{CM} + mb^2$. *Perpendicular axis theorem:* $I_x = I_y + I_z$. $I_{sphere} = \frac{2}{5}ma^2$. $I_{cylinder} = \frac{1}{2}ma^2$. $I_{plate} = \frac{1}{12}m(a^2 + b^2)$. $I_{rod} = \frac{1}{12}mL^2$ (center of mass).

Rotation in space: $\Omega = \sum m_\mu(r_\mu \times (\omega \times r_\mu))$, $[(r_\mu \times (\omega \times r_\mu)]_x = {\omega_x}({y_\mu}^2 + {z_\mu}^2) - \omega_y x_\mu y_\mu - \omega_z x_\mu z_\mu$, $I_{xx} = \int(y^2 + z^2)dm$, $I_{xy} = -\int(xy)dm$, $\mathcal{I} = \begin{pmatrix} I_{xx} & I_{xy} & I_{xz} \\ I_{yx} & I_{yy} & I_{yz} \\ I_{zx} & I_{zy} & I_{zz} \end{pmatrix}$ is the *inertia tensor.* $T = \frac{1}{2}\omega \cdot \Omega$ is kinetic energy. *Principal Axis Theorem:* If $\omega_1, \omega_2, \omega_3$ and $\Omega_1, \Omega_2, \Omega_3$ are the angular velocities and momenta about the principal axis, $\Omega_i = I_i\omega_i$ and $T = \frac{1}{2}(I_1\omega_1^2 + I_2\omega_2^2 + I_3\omega_1^3)$. *Ellipsoid of rotation:* Let $\hat{n}$ be a unit vector in the direction of $\hat{\omega}$, $\vec{\omega} = \hat{n}\omega = \omega(icos(\alpha) + jcos(\beta) + kcos(\gamma))$. $T = \frac{1}{2}I\omega^2$ where $I = I_{xx}cos^2(\alpha) + I_{yy}cos^2(\beta) + I_{zz}cos^2(\gamma) + 2I_{xy}cos(\alpha)cos(\beta) + 2I_{xz}cos(\alpha)cos(\gamma) + 2I_{yz}cos(\beta)cos(\gamma)$. $\rho = \frac{\hat{n}}{\sqrt{I}}$ is ellipsoid of revolution. *Rotational symmetry about $s = z$ axis:* $I_s = I_z$, $I = I_x = I_y$. $I\dot{\omega}_x + \omega_y\omega_z(I_s - I) = 0$, $I\dot{\omega}_y + \omega_x\omega_z(I - I_s) = 0$, $I_s\dot{\omega}_z = 0$. $\vec{J}_s = const$, put $\gamma = \frac{I_s - I}{I}\omega_s$; then $\dot{\omega}_x + \gamma\omega_y =$, $\dot{\omega}_y - \gamma\omega_x =$, so $\ddot{\omega}_x + \gamma^2\omega_x = 0$ and $T_p = \frac{2\pi}{\gamma}$. *Precession of Earth:* $T_p = \frac{2\pi I}{\omega_z(I_s - I)} \approx 305days$. *Precession of Disc:* $T_p = \frac{2\pi}{\omega_z}$.

Gyroscope: $J_{x'} = I_{x'}\omega_{x'} = I\dot{\theta}$, $J_{y'} = I\varphi sin(\theta)$, $J_{z'} = I_s S$. $S = \dot{\varphi}cos(\theta) + \dot{\phi}$, $I_s\dot{S} = 0$.

Euler's equations: Let O be a principal axis coordinate system fixed in a body, the external torque is $\vec{\Lambda}$. $I_1\dot{\omega}_1 + (I_3 - I_2)\omega_2\omega_3 = \Lambda_1$, $I_2\dot{\omega}_2 + (I_1 - I_3)\omega_1\omega_3 = \Lambda_2$, $I_3\dot{\omega}_3 + (I_2 - I_1)\omega_1\omega_2 = \Lambda_3$ along the principal axes. $\omega \cdot \Omega = c$ is invariant plane. The angular velocity and momentum in terms of the Euler angles ϕ, θ, ψ, from O_{xyz} fixed in space to $O_{x'y'z'}$ is: $\omega_{x'} = \dot{\phi}sin(\theta)sin(\psi) + \dot{\theta}sin(\psi)$, $\omega_{y'} = \dot{\phi}sin(\theta)cos(\psi) - \dot{\theta}sin(\psi)$, $\omega_{z'} = \dot{\phi}cos(\theta) + \dot{\psi}$, ϕ is from x to line of nodes, θ is from z to z' axis, and, ψ is from line of nodes to x'; $T = \frac{1}{2}(I_1{\omega_1}^2 + I_2{\omega_2}^2 + I_3{\omega_3}^2)$. *Top:* Suppose $\vec{e}_3$ is the axis of top's line of symmetry. $\vec{s} = s\vec{e_3} = \dot{\psi}\vec{e_3}$. $\Omega = I_1\omega_1 e_1 + I_2\omega_2 e_2 + I_3(\omega_3 + s)e_3$, $\Lambda = le_3 \times mg = (\frac{d\Omega}{dt})_F, I_1 = I_2$. $(\frac{d\Omega}{dt})_F = (\frac{d\Omega}{dt})_B + \omega \times \Omega$. $I_1\dot{\omega}_1 + (I_3 - I_2)\omega_2\omega_3 = mglsin(\theta)$, $I_2\dot{\omega}_2 + (I_1 - I_3)\omega_1\omega_3 - I_3\omega_1 s = 0$, $I_3(\dot{\omega}_3 + \dot{s}) = 0$. In Euler angles, with $\psi = 0$, this is $\omega_1 = \dot{\theta}$, $\omega_2 = \dot{\psi}sin(\theta)$, $\omega_3 = \dot{\psi}cos(\theta)$. $\dot{\theta}, \dot{\psi}, s$ are angular velocity of precession, nutation and spin.

Hamilton-Lagrange and variational methods: *Holonomic constraint:* $\phi(q_1, q_2, ..., q_n, t) = 0$. *Generalized coordinates:* $\delta W = \sum_\alpha \Phi_\alpha \delta q_\alpha$, $\Phi_\alpha = \sum \vec{f} \cdot \frac{\partial r}{\partial q_\alpha}$. *Lagrange equations:* $(\frac{d}{dt})\frac{\partial T}{\partial \dot{q}_\alpha} - \frac{\partial T}{\partial q_\alpha} = \Phi_\alpha$. If the forces are all conservative and $L = T - V$ then $(\frac{d}{dt})\frac{\partial L}{\partial \dot{q}_\alpha} - \frac{\partial L}{\partial q_\alpha} = 0$. *Generalized momentum:* $p_\alpha = \frac{\partial T}{\partial \dot{q}_\alpha}$. *Hamilton:* $H(p_1, ..., p, q_1, ..., q_n, t) = \sum p_\alpha \dot{q_\alpha} - L$. $\dot{p_\alpha} = -\frac{\partial H}{\partial q_\alpha}$, $\dot{q_\alpha} = \frac{\partial H}{\partial p_\alpha}$. *Hamilton Principal:* For conservative forces ($H = T + V$), $L = T - V$, $\delta \int_{t_1}^{t_2} L dt = 0$. Note: $H = \sum p_\alpha \dot{q_\alpha} - L$. *Modern setting:* $S = \int_{t_1}^{t_2} L(q_i, \dot{q}_i)\, dt$. $L(x_i, \dot{x}_i) = \frac{m}{2}\dot{x}_i^2 - V(x_i)$. If L is independent of q_i, $p_i = \frac{\partial L}{\partial \dot{q}_i}$ is conserved. $H(q_i, p_i) = p_i\dot{q}_i - L(q_i\dot{q}_i)$, this can be expressed in terms of $q_i, \dot{q}_i$ provided $[\frac{\partial^2 L}{\partial \dot{q}_i \partial \dot{q}_j}]_{ij}$ is invertible. $dH = \dot{q}_i dp_i - \frac{\partial L}{\partial q_i} dq_i$. On Euler trajectory, $\frac{\partial H}{\partial p_i} = \dot{q}_i$ and $\frac{\partial H}{\partial q_i} = -\dot{p}_i$, H is conserved. Let $A(q, p)$ be a function. $\frac{dA}{dt} = \frac{\partial A}{\partial q}\frac{\partial H}{\partial p} - \frac{\partial A}{\partial p}\frac{\partial H}{\partial q} = [A, H]$. This is the *Poisson bracket*; $[q_i, q_j] = [p_i, p_j] = 0$ and $[p_i, q_j] = \delta_{ij}$. Under $T : q_i \mapsto q_i + \epsilon f_i(q)$, $Q = p_i f_i(q)$ is conserved and $[q_j, Q] = f_j(q)$, $\delta q_j = \epsilon[q_j, Q]$; the conserved quantity is a generator of the symmetry.

4.3 Thermodynamics and Statistical Mechanics

Rubric for Statistical Mechanics: Consider a system with total energy E^* consisting of two subsystems A and A' in thermal equilibrium. Suppose A has energy E and A' has energy $E' = E^* - E$. Let $\Omega^*(E)$ be the number of states accessible to the system when A has energy E then $\Omega^*(E) = \Omega(E)\Omega(E')$. If $P(E)$ is the probability of having A in energy state E, $P(E) = C\Omega^*(E) = C\Omega(E)\Omega'(E')$. Thermal equilibrium favors the largest number of accessible states. This happens when $P(E)$ and hence $ln(P(E))$ is maximum or when $\frac{\partial ln(P(E))}{\partial E} = 0$ or equivalently when $\frac{\partial ln(\Omega(E))}{\partial E} + \frac{\partial ln(\Omega'(E'))}{\partial E} = 0$. This occurs when $\beta(E) = \frac{1}{\Omega(E)}\frac{\partial \Omega(E)}{\partial E} = \frac{1}{\Omega'(E')}\frac{\partial \Omega(E')}{\partial E'} = \beta'(E')$. $\beta(E)$ characterizes the temperature and we define $\beta(E) = \frac{1}{kT}$. Putting $S = kln(\Omega)$, $\frac{1}{kT} = \frac{\partial S}{\partial E}$. For distribution of states, imagine A is in start r with energy E_r. $P(E_r)\Omega'(E^* - E_r)$. By Taylor, $ln(\Omega(E^* - E_r)) = ln(\Omega(E^*)) - \frac{\partial \Omega}{\partial E}E_r$ and we get the familiar $P(E_r) = Ce^{-\frac{E_r}{kT}}$.

Basic pattern: In canonical ensemble, $\langle E \rangle$ and the number of particles, N, is fixed. In *grand canonical ensemble*, $\langle E \rangle$ and $\langle N \rangle$ are fixed. Let $|i\rangle$ be the microstates; $\sum a_i = A$, $\sum_i a_i E_i = AE$; the number of configurations is $W(\vec{a}) = \frac{A!}{\prod_i a_i!}$ and $P_i = \frac{a_i}{A}$. To find $\langle \overline{a_i} \rangle$, maximize $ln(W(\vec{a}))$, we use Lagrange multipliers and the two constraints, namely, solve $L(\vec{a}) = ln(W(\vec{a})) + \alpha(A - \sum_i a_i) + \beta(AE - \sum_i a_i E_i) = 0$ and $\frac{\partial L(\vec{a})}{\partial a_j} = 0$. Systems in thermal equilibrium have same $\beta = \frac{1}{kT}$. $Z = \sum_i e^{-\beta E_i}$ and $\langle E \rangle = \frac{\partial Z}{\partial \beta}$. $dE = TdS - PdV$. $\beta\mu = -\gamma$ is the chemical potential.

First law: ΔQ: heat into system, If ΔW: work on system, ΔE: increase in energy of system then $\Delta Q + \Delta W = \Delta E$. For ideal gas, $PV = E = \frac{2}{3}N\langle\frac{mv^2}{2}\rangle = nRT = NkT$. In general, $PV = (\gamma - 1)U$ ($\gamma = \frac{5}{3}$ for ideal gas). $(\frac{\partial U}{\partial T})_V = C_v = \frac{3}{2}R$, $(\frac{\partial U}{\partial T})_p = C_p = C_v + R$, for adiabatic process: $pV^\gamma = c$, $\gamma = \frac{C_P}{C_V}$.

Second Law: It is impossible to build a cyclic engine that converts thermal energy completely into mechanical work.

Carnot Process: $1 \to 2$: gas placed on hot reservoir at T_H adding Q_H, isothermally; $2 \to 3$: gas expands and does work adiabatically; $3 \to 4$: gas placed on cold reservoir at T_C, removing heat Q_C isothermally; $4 \to 1$: work done on gas adiabatically. $e = 1 - \frac{T_C}{T_H}$. For reversible process, $S = \int \frac{dQ}{T} \geq 0$. $S = Nk_B ln(\Omega)$. In irreversible process, entropy increases, at $T = 0$, $S = 0$. For reversible process, $S = \frac{Q_1}{T_1} = \frac{Q_2}{T_2}$, $W = Q_1 - Q_2 = Q_1(1 - \frac{T_2}{T_1})$; eff $= \frac{W}{Q_1} = \frac{T_2 - T_1}{T_1}$. $S = kln(W)$. $e = 1 - \frac{T_C}{T_H}$. $(c_v)_{\text{monatomic}} = \frac{3}{2}R$, $(c_v)_{\text{diatomic}} = \frac{5}{2}R$, $(c_p)_{\text{monatomic}} = \frac{5}{2}R$.

Statistical Mechanics: For *monatomic gas*, $P = \frac{2}{3}U = (\gamma - 1)U = \frac{2}{3}\langle mv^2\rangle = \frac{3}{2}kT$. In a mixture at constant temperature with two species 1 and 2, $n_1\langle {m_1 v_1}^2\rangle = n_2\langle {m_2 v_2}^2\rangle$ but considering two particles with relative velocity w with velocity of enter of mass v_{CM} we can argue at equilibrium that $\langle w \cdot V_{CM}\rangle = 0$ so $n_1 = n_2$ (Avogadro's hypothesis). $v_{\text{rms}} = \sqrt{\frac{3RT}{M}}$. For *photon gas*, $PV = N\langle p \cdot v\rangle/3$ so $\gamma = \frac{4}{3}$. For a *diatomic gas* $\gamma = \frac{9}{7}$. $S = kln(W)$, $\Delta S = kln(\frac{W_f}{W_i})$ and $\frac{\partial S}{\partial E} = \frac{1}{T}$ and $\Delta S = \int_i^f \frac{dQ}{T}$. $N_M(E_n) = NAe^{-E_n/kT}$ and $D(E) = \frac{dn}{dE}$. $dN = N \times DdE$. For Bosons: $D_B(E) = \frac{8\pi V}{h^3c^3}E^2$. For $E_{internal} = \int_0^\infty E\frac{1}{e^{E/kt}-1}\frac{8\pi V}{h^3c^3}E^2dE = \frac{8\pi k}{15h^3c^3}VT^4$. $C_v = \frac{\partial E_{internal}}{\partial T}$. For insulators, $C_v = 3R$ and for conductors, $C_v = \frac{9}{2}R$. $F = E - TS$. For ideal gas, $C_v = \frac{3}{2}R$. $Z = \sum_j e^{\beta E_j}$ and $\langle E\rangle = -\frac{\partial ln(Z)}{\partial \beta}$. If $I_n = \int_0^\infty e^{-\alpha x^2}x^2dx$ then $I_n = \frac{n-1}{2\alpha}I_{n-2}$.

Atmosphere: $\frac{dn}{dh} = -\frac{mg}{kT}n$, $n = n_0e^{-PE/kT}$ and $\frac{n_{>u}}{n_{<u}} = e^{-KE/kT}$. *Evaporation model:* W is binding energy of liquid, n is density of vapor, $1/V_a$ is density of liquid then $nV_a = e^{-W/kT}$. *Chemical kinetics:* $\frac{n_An_B}{n_{AB}} = ce^{W/kT}$. *Diffusion:* Average time to collision is $\frac{1}{n_0}\int_0^\infty t\frac{N(t)dt}{\tau}$, $N = N_0e^{t/\tau}$. *Mean Free Path:* $l = \tau v = \frac{1}{n\sigma}$; for dilute gas, $l = \frac{RT}{\sqrt{2}\pi d^2N_AP}$. *Thermal conductivity:* $\frac{1}{A}\frac{dQ}{dt} = -\kappa\frac{dT}{dz}$, $\kappa = \frac{knlv}{\gamma - 1}$ if $MFP <<$ container.

Maxwell Distribution: $F_{MB} = N(\frac{m}{2\pi kT})^{\frac{3}{2}}e^{-m(v_x^2+v_y^2+v_z^2)/(2kT)}$, the frequency of a particle around v; $dn_\nu = F_{MB}g(q)dq$. $v_{rms} = \sqrt{\frac{3kT}{m}}$.
Bose-Einstein Distribution (Bosons): $F_{BE} = (e^\alpha e^{E_i/kT} - 1)^{-1}$, α is type specific 0 for photon.
Fermi-Dirac Distributions (Fermions): $F_{FD} = (e^{(E_i - E_f)/kT} + 1)^{-1}$, E_f is the *Fermi energy*. $C_V = \frac{1}{N}(\frac{\partial E}{\partial T})_V$ approximately $3R$ for many solids.

Definitions: *Conductor:* half filled conduction band. *Insulator:* filled conduction band large gap $\approx 5ev$. *Semiconductor:* filled conduction band small gap $\approx 1ev$ which can be overcome by thermal excitation. *Electron mobility:* $\mu = \frac{v_d}{E}$, v_d is drift velocity. *Fine constant:* $\frac{ke^2}{\hbar c} \approx \frac{1}{137}$. *Josephson junction* is two superconductors separated by thin $\approx 1nm$ insulator; if there is no potential difference, electrons tunnel and we get dc, if dc potential is applied, we get ac with $f \approx \frac{2eV}{h}$.

4.4 Quantum Mechanics

Schrodinger and its discontents: $-\frac{\hbar^2}{2m}\frac{\partial^2\Psi(x,t)}{\partial x^2} + U\Psi(x,t) = i\hbar\frac{\partial\Psi(x,t)}{\partial t}$, $\int_S |\Psi|^2 = 1$. $\langle Q(x,p)\rangle = \int \Psi^* Q(x, \frac{\hbar}{i}\frac{\partial}{\partial x})\Psi dx$. $\hat{H} = -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2} + V(x)$. Separation of variables (for well defined energy): $\Psi(x,t) = \varphi(x)\phi(t)$. $-\frac{\hbar^2}{2m}\varphi''(x)\phi(t) + U\varphi(x)\phi(t) = i\hbar\varphi(x)\dot{\phi}(t)$. So $-\frac{\hbar^2}{2m}\frac{\varphi''(x)}{\varphi(x)} + U = E = i\hbar\frac{\dot{\phi}(t)}{\phi(t)}$. $\phi(t) = Ae^{-i(E/\hbar)t}$, $E = \hbar\omega$. $E = K + U$; system is *bound* if $K_0 < U_0$. The remaining time-independent equation is $\varphi'(x) = k^2(V-E)\varphi(x), k^2 = \frac{2m(V-E)}{\hbar^2}$. If $V - E > 0$ (bound states), the solution is $\varphi(x) = Ae^{kx} + Be^{-kx}$. If $V - E < 0$ (scattering), the solution is $\varphi(x) = Ae^{ikx} + Be^{-ikx}$ or $\varphi(x) = Acos(kx) + Bsin(kx)$. Note that for solution when separation of variables is possible, $|\Psi|^2$ is time independent. If $Q(x,p)$ is an operator, $\langle Q\rangle = \frac{i}{\hbar}\langle [H,Q] + \langle\frac{\partial Q}{\partial t}\rangle\rangle$. Consider the usual harmonic potential $V(x) = \frac{1}{2}m\omega^2x^2$ in Schroedinger's equation: $\frac{1}{2m}[\frac{\hbar}{i}\frac{d^2\Psi}{dx^2} + \frac{1}{2}m^2\omega^2x^2\Psi] = E\Psi$. Define $a_\pm = \frac{1}{\sqrt{2m}}(\frac{\hbar}{i}\frac{d}{dx} \pm im\omega x)$. $a_+a_- = \frac{1}{2m}[\frac{\hbar}{i}\frac{d^2\Psi}{dx^2} + \frac{1}{2}m^2\omega^2x^2\Psi] - \frac{1}{2}\hbar\omega$. If Ψ solves the Schroedinger equation with energy E, $a_+\Psi$ solves the Schroedinger equation with energy $E+\hbar\omega$.

Potential well: Region 1: $x < 0, U = U_0$; Region 2: $0 \le x \le L, U = 0$; Region 3: $x > L, U = U_0$. For infinite potential, applying $\varphi_1(0) = \varphi_2(0) = 0$, $\varphi_2(L) = \varphi_3(L) = 0$ leads to quantization, $\sqrt{\frac{2mE}{\hbar^2}} = n\pi$, $E_n = \frac{n^2\pi^2\hbar^2}{2mL^2}$, $\varphi_n(x) = \sqrt{\frac{2}{L}}sin(\frac{n\pi x}{2})$. E_0 is the ground state. For finite potential with bound states ($V > E$), $\varphi_1(x) = A_1e^{k_1x} + B_1e^{-k_1x}$, $\varphi_2(x) = A_2cos(k_2x) + B_2sin(k_2x)$, $\varphi_3(x) = A_3e^{k_3x} + B_3e^{-k_3x}$ with $\varphi_1(0) = \varphi_2(0)$, $\varphi_2(L) = \varphi_3(L)$ and $\varphi_2'(0) = \varphi_3'(0)$, $\varphi_2'(L) = \varphi_3'(L)$. Due to square integrable condition, $B_1 = A_3 = 0$. $k_1^2 = \frac{2m(V-E)}{\hbar^2} = k_3^2 = k$ and $k_2^2 = \frac{2m(E)}{\hbar^2} = \kappa^2$. Solutions are even or odd. For even solutions, $B_2 = 0$. Applying boundary condition, $B_3e^{-kL} = A_3cos(\kappa L)$ and $-kB_3e^{-kL} = -\kappa A_3sin(\kappa L)$. Dividing the two equations gives $k = \kappa tan(\kappa L)$.

Free Particle: $\varphi''(x) = -k^2\varphi$, $k^2 = \frac{2mE}{\hbar^2}$. $\varphi(x) = Ae^{i(kx+\frac{\hbar k^2}{2m}t)}Be^{i(kx-\frac{\hbar k^2}{2m}t)}$. There is no solution for free particle with definite energy E but $\Psi(x,t) = \frac{1}{\sqrt{2m}}\int_\infty^\infty \psi(k)e^{i(kx-\omega t)}dk$, $\omega = \frac{\hbar k^2}{2m}$.

Dispersion is the relationship between frequency (ω) and wave number (k). Examples: $v_{phase} = \frac{\omega}{k}$ for EM waves, $v_{phase} = \frac{\omega}{k} = \frac{mc^2}{\hbar k} + \frac{\hbar k}{2m}$ for matter waves. $v_{group} = \frac{d}{dk}(ck) = c$ for EM waves, $v_{group} = \frac{d}{dk}(\frac{mc^2}{\hbar k} + \frac{\hbar k}{2m}) = \frac{\hbar k_0}{m}$ for matter waves. Transmission rate for matter waves through potential barrier is $\frac{sinh^2(\alpha L)}{sinh^2(\alpha L) + \frac{\alpha^2k^k}{(k^2+\alpha^2)^2}}$. Reflection rate for matter waves through potential barrier is $\frac{(k^2+\alpha^2)^2}{sinh^2(\alpha L) + \frac{\alpha^2k^k}{(k^2+\alpha^2)^2}}$.

Resonant transmission: $E = U_0 + \frac{n^2\pi^2\hbar^2}{2mL^2}$. $n_{plasma} = \sqrt{1 - \frac{\omega_p^2}{\omega\omega_m}}, \omega_m = \frac{eB_0}{m}$. $v_pv_g = c^2$.

Hydrogen atom: In polar coordinates, $\nabla^2 = \frac{1}{r^2}[\frac{\partial}{\partial r}(r^2\frac{\partial}{\partial r}) + csc(\theta)\frac{\partial}{\partial\theta}(sin(\theta)\frac{\partial}{\partial\theta}) + csc^2(\phi)\frac{\partial^2}{\partial\theta^2}]$. For H, $\phi(r,\theta,\phi) = R(r)\Theta(\theta)\Phi(\phi)$. Schroedinger becomes $\frac{1}{R}\frac{\partial}{\partial r}(r^2\frac{\partial R}{\partial r}) + \frac{1}{\Theta}csc(\theta)\frac{\partial}{\partial\theta}(sin(\theta)\frac{\partial\Theta}{\partial\theta}) + csc^2(\phi)[\frac{1}{\Phi}\frac{\partial^2\Phi}{\partial\theta^2}] = -r^2\frac{2m(E-U(r))}{\hbar^2}$. To solve, note that $\frac{1}{\Phi}\frac{\partial^2\Phi}{\partial\theta^2} = c_\phi$ whose solution is $\Phi(\phi) = e^{im_l\phi}, m_l 0, \pm1, \ldots$ and $c_\phi = -(m_l)^2$. m_l is the *magnetic quantum number*. After substitution, this becomes $\frac{1}{R}\frac{\partial}{\partial r}(r^2\frac{\partial R}{\partial r}) + \frac{1}{\Theta}csc(\theta)\frac{\partial}{\partial\theta}(sin(\theta)\frac{\partial\Theta}{\partial\theta}) + csc^2(\phi)(-m_l^2) = -r^2\frac{2m(E-U(r))}{\hbar^2}$ and $\frac{1}{\Theta}csc(\theta)\frac{\partial}{\partial\theta}(sin(\theta)\frac{\partial\Theta}{\partial\theta}) = c_\theta$ leads to $c_\theta = -l(l+1), |m_l| \le l$ and $\Theta_{l,m_l}(\theta) = P_{l,m_l}(cos(\theta))$, $|L| = \hbar\sqrt{l(l+1)}$. l is the *orbital quantum number*. $L_z = m_l\hbar$. Finally, we must solve $\frac{1}{R}\frac{\partial}{\partial r}(r^2\frac{\partial R}{\partial r}) - l(l+1) = -r^2\frac{2m(E-U(r))}{\hbar^2}$ and $E = \frac{-me^4}{2(4\pi\epsilon_0)^2\hbar^2}\frac{1}{n^2}$, $0 \le l < n$. n is the *principal quantum number*. $E_n = \frac{-13.6 \text{ ev}}{n^2}$. $r \approx n^2a_0, a_0 = \frac{4\pi\epsilon_0\hbar^2}{m_l^2}$. Some of the solutions are:

n,l	$R_{n,l}(r)$
$1,0$	$\frac{1}{(a_0)^{\frac{3}{2}}}e^{-r/a_0}$
$2,0$	$\frac{1}{2(a_0)^{\frac{3}{2}}}2(1-\frac{r}{2a_0})e^{-r/(2a_0)}$
$2,1$	$\frac{1}{2(a_0)^{\frac{3}{2}}}(\frac{4\sqrt{2}r}{9a_0})e^{-r/(2a_0)}$
$3,0$	$\frac{1}{3(a_0)^{\frac{3}{2}}}(2-\frac{4r}{3a_0}+\frac{4r^2}{27a_0^2})e^{-r/(3a_0)}$

and correspondingly,

l,m_l	$\Theta_{l,m_l}(\theta)\Phi_{m_l}(\phi)$
$0,0$	$\frac{3}{4\pi}$
$1,0$	$\frac{4}{4\pi}cos(\theta)$
$1,\pm1$	$\frac{3}{8\pi}sin(\theta)e^{\pm i\phi}$
$2,0$	$\frac{5}{16\pi}(3cos^2(\theta)-1)$
$2,\pm1$	$\frac{15}{8\pi}cos(\theta)sin(\theta)e^{\pm i\phi}$

.

Spin adds intrinsic angular momentum: $S=\sqrt{s(s+1)}\hbar$. Electron has spin $s=\pm\frac{1}{2}$. Spin state is m_s. *Stern Gerlach:* $F=\mu_z\frac{\partial B_z}{\partial z}\hat{z}$, $\mu_z=-\frac{e}{2m_l}L_z$. $S_z=S\hbar$.

Multiparticle systems: $\frac{-\hbar^2}{2m}(\frac{\partial^2\phi(x_1,x_2)}{\partial x_1^2}+\frac{\partial^2\phi(x_1,x_2)}{\partial x_2^2})+U\phi(x_1,x_2)=E\phi(x_1,x_2)$. First problem is interparticle force but even without that, say two identical particles react only to external forces, we have $\frac{-\hbar^2}{2m}(\frac{\partial^2\phi_1(x_1)}{\partial x_1^2}+U(x_1)\phi_1(x_1)+\frac{\partial^2\phi_2(x_2)}{\partial x_2^2})+U\phi(x_2)=E_1\phi_1(x_1)+E_2\phi_2(x_2)$. Then $C_1=\frac{n_1^2\pi^2\hbar^2}{2mL}$ and $C_2=\frac{n_2^2\pi^2\hbar^2}{2mL}$. The combined wave function is $\phi(x_1,x_2)=\phi_1(x_1)\phi_2(x_2)$. Depending on n_1 and n_2, one particle could have probability 0 at a location and the other non-zero probability. But then particles can be distinguished which violates *exchange symmetry*. Thus the wave function must be "symmetrized" as either (a) $\phi_S(x_1,x_2)=\phi_1(x_1)\phi_2(x_2)+\phi_2(x_1)\phi_1(x_2)$, or (b) $\phi_A(x_1,x_2)=\phi_1(x_1)\phi_2(x_2)-\phi_2(x_1)\phi_1(x_2)$. The general multiparticle Schroedinger becomes $\frac{-\hbar^2}{2m}\sum_i\nabla_i^2\phi(r_1,\ldots,r_n)+\sum_{i<j}U(|r_i-r_j|)+\sum_i U_i(|r_i-r_j|)=E\phi(r_1,\ldots,r_n)$. *Hartree Model:* $Z(r)=1+(Z-1)e^{-br}$.

Spin orbit interaction: $U=\vec{\mu}_S\cdot\vec{B}_L=(-g_e\frac{e}{2m_e}\vec{S})\cdot\frac{\mu_0 e}{4\pi m_e r^3}$. $\vec{J}=\vec{L}+\vec{S}$. Spin is a relativistic effect, $L=\sqrt{l(l+1)}\hbar$ and $S=\sqrt{s(s+1)}\hbar$. $\alpha=\frac{e^2}{(4\pi\epsilon_0)\hbar c}=\frac{1}{137}$.

Formalism: Let $|i\rangle$ denote base states $\langle i|j\rangle=\delta_{ij}$. $|\psi\rangle=\sum_i|i\rangle\langle i|\psi\rangle$, $\langle\psi|\phi\rangle=\sum_i\langle\phi|i\rangle\langle i|\psi\rangle$. $|\psi\rangle=\sum_i|i\rangle\langle i|\psi\rangle$ evolves under $\hat{A}$ so $|\phi\rangle=\hat{A}|\psi\rangle$ and $\langle i|\phi\rangle=\sum_j\langle i|\hat{A}|j\rangle\langle j|\psi\rangle$, $A_{ij}=\langle i|\hat{A}|j\rangle$.

Observables: Suppose $\hat{Q}f=\lambda f$, then $\Delta Q=0$ iff $\hat{Q}\Psi=\overline{Q}\Psi$. For momentum, $\hat{p}e^{ikx}=-i\hbar\frac{\partial}{\partial x}e^{ikx}=\hbar ke^{ikx}$; note that the eigenvalues are $p=\hbar k$. The observable with eigenvalue a_n has $P(a_n)=\sum_{i=1}^{g_n}|\langle u_n^i|\Psi\rangle|^2$. Density operator is $\rho=|\Psi\rangle\langle\Psi|$.

Quantum mechanical operators: $\int_{\mathbb{R}^3}|\psi(\vec{x})|d\vec{x}=1$. *Spatial operators:* $X\psi=x\psi$, $Y\psi=y\psi$, $Z\psi=z\psi$, $\vec{R}=(X,Y,Z)$. *Momentum operators:* $p_x\psi=-\frac{\hbar}{i}\frac{\partial}{\partial x}\psi$, $p_y\psi=-\frac{\hbar}{i}\frac{\partial}{\partial y}\psi$, $p_y\psi=-\frac{\hbar}{i}\frac{\partial}{\partial z}\psi$, $\vec{P}=(p_x,p_y,p_z)$. *Angular Momentum:* $L_x=yp_z-zp_y$, etc. $\langle A\rangle=\int\psi^*(\vec{r})A\psi(\vec{r})d\vec{r}$, $\Delta A=\sqrt{\langle A^2\rangle-\langle A\rangle^2}$. *Time:* $T\psi=t\psi$. *Energy:* $E\psi=\frac{\hbar}{i}\frac{\partial}{\partial t}\psi$.

Axiomatics for Quantum Mechanics: Elements of state space are denoted: $|\varphi\rangle$ and $(\phi,\psi)=\langle\phi|\psi\rangle=\overline{\langle\psi|\phi\rangle}$, physically observable quantities are described by hermitian operators acting on state space: $A|\psi\rangle$, each observable quantity is an eigenvalue of the hermitian operator.

Postulate 1: Associated with any *isolated* physical system is a complex vector space, V with an inner product called a state space. The system is completely described by $v \in V$.

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation on the state: $|\psi(t_2)\rangle = U|\psi(t_1)\rangle$. *Postulate 2':* The non-relativistic evolution of a closed quantum system is described by Schroedinger's equation $i\hbar\frac{\partial|\psi\rangle}{\partial t} = H|\psi\rangle$.

Postulate 3: Quantum measurements are described by a collection of measurement operators, $\{M_m\}$ that act on the state space. If $|\psi\rangle$ is the state immediately before the measurement, the probability that the event m occurs is $\langle\psi|M_m^\dagger M_m|\psi\rangle$ and the state after the measurement is given by $\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$ and M_m satisfies $\sum_m M_m^\dagger M_m = I$. A projective measurement on an observable with spectral decomposition, $M = \sum_m mP_m$, results in one of the m values as possible outcomes. $\Delta(C)\Delta(D) \geq \frac{\langle\psi|[C,D]|\psi\rangle}{2}$.

Postulate 4: The state space of a composite system is the tensor product of the state spaces of the component systems. If we number the systems $1, 2, \ldots, n$, and system i is in the prepared state $|\psi_i\rangle$ then the joint state is $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$.

Simple quasi-classical operators: *Harmonic oscillator:* $H = \frac{p^2}{2m} + k\frac{x^2}{2}$. *EM Hamiltonian:* $H = \frac{1}{2m}(p - \frac{q}{c}A)^2 + V(R) + q\phi - \frac{q}{mc}S \cdot B, B = \nabla \times A$. Simultaneously observable quantities commute. *Independence and uncertainty:* $[R_j, P_k] = i\hbar\delta_{jk}, [R_j, R_k] = 0$.

Feynman Postulates: If there is no spin or polarization: (1) $\langle x|s\rangle = a + bi$. $Pr($ particle arrives at $x|$ particle leaves $s) = |\langle x|s\rangle|^2$. (2) $\langle x|s\rangle_{both} = \langle x|s\rangle_1 + \langle x|s\rangle_2$. (3) $\langle x|s\rangle_{via\ 1} = \langle x|1\rangle\langle 1|s\rangle$. a is probability light scattered at 1 arrives at D_1 and b that it arrives at D_2 ($a >> b$). $\langle\vec{r_2}|\vec{r_1}\rangle = \frac{A}{r_{12}}e^{i\frac{\vec{p}\cdot\vec{r}_{12}}{\hbar}}$; get p relativistically by $(pc)^2 = E^2 - (m_0c^2)^2$ or non-relativistically as $E = \frac{p^2}{2m}$. Rules for outcomes: (1)If final states are distinguishable, add probabilities *not amplitudes* for indistiguisible processes leading to the same final state add *amplitudes*; (2) use complete description of isolates system. Outcome of scattering with indistinuishable particles always exhibit interference: add amplitudes for *Bosons,* subtract for *Fermions.* $P_n(Bose) = n!P_n(\text{different})$. Treat metal conduction as noninteracting Fermion gas.

4.5 More Quantum

Polar Decomposition: Let A be a linear operator on V. Then there is a unitary operator U and positive operators J, K: $A = UJ = KU$. $J = \sqrt{A^TA}$, $K = \sqrt{AA^T}$. **Singular Value Decomposition:** Let A be a square matrix the $\exists U, V$ and a diagonal matrix D with non-negative entries such that $A = UDV$. Entries of D are called singular values. **Schmidt decomposition:** If $|\Psi\rangle$ is a vector in the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ there are orthonormal bases $\{\varphi_i^A\}$ and $\{\varphi_i^B\}$ such that $\Psi = \sum\sqrt{p_i}|\varphi_i^A\rangle|\varphi_i^B\rangle$.

Standard Model: Quantized force fields materialize as particles. Matter particles: *Fermions* (half-integral spins). Force particles: *Bosons* (integral spins). u: $q = +\frac{2}{3}$, $m = 2Mev$; d: $q = -\frac{1}{3}$, $m = 5Mev$; c: $q = +\frac{2}{3}$, $m = 1.25Gev$; s: $q = -\frac{1}{3}$, $m = 95Mev$; t: $q = +\frac{2}{3}$, $m = 171Mev$; b: $q = -\frac{1}{3}$, $m = 4.2Gev$.
ν_e: $q = 0$; ν_μ: $q = 0$; ν_τ: $q = 0$. e: -1, $m = .511Mev$; μ: -1, $m = 106Mev$; τ: 0, $m = 1.78Gev$. Bosons: Photon γ - EM Force: $q = 0$, $m = 0$; Gluons - Strong Force: $q = 0$, $m = 0$; Z - weak force: $q = 0$, $m = 91Gev$; W^+, W^- - weak force: $q = 0$, $m = 80.4Gev$; Higgs (H): $q = 0$, $114Gev < m < 192Gev$; Graviton - gravity: $q = 0$, $m = 0$.

Type	Family 1	Family 2	Family 3
Quark	Up (u)	Charm (c)	Top (t)
Quark	Down (d)	Strange (s)	Bottom (b)
Lepton	electron neutrino (ν_e)	muon neutrino (ν_μ)	Tau neutrino (ν_τ)
Lepton	electron (e)	muon (μ)	Tau (τ)

Figure 4.5: Matter Particles - Fermions - not including antiparticles

Hall Effect: In metal or semiconductor, imagine a thin ($2D$) slab, z-up, x-across, y-back, with an electric field, $\vec{E}_y$, back, current $\vec{j}_x$ across. Turn on a magnetic field $\vec{B}_z$, and the charges move to the back until equilibrium caused by electrostatic build-up when $B_z v_x = E_y$, then Hall resistance is $R_H = \frac{E_y}{B_z} j_x$, $j_x = v_x N_q$. At low temperature ($< 30mK$), a quantum effect appears: R_H grows monotonically with B_z and is quantized by $\frac{1}{n}\frac{h}{e^2}$; this IQHE is evident in a GaAs-GaAlAs hetero-juncture. The magnetic field shifts the Landau Levels. The diagonal resistance R_{xx} is at times 0 when the *Fermi energy* of the electrons lies between the *Landau Levels* freezing out scattering. (The Fermi energy, E_F, is the energy of the fermion composite at $0K$.) When the mobility of the electrons is high, additional plateaus (corresponding to $R_{xx} = 0$) appear; this is due to electron interaction giving rise to fractional charge like quasi-particles; this is the FQHE. Unlike IQHE, the FQHE gives rise to non-Abelian statistics in the gapped degenerate states.

Fractional Quantum Hall Physics: *Laughlin wave function:* $\Phi^m(z_1, \ldots, z_n) = \prod_{i<j}(z_i - z_j)^m e^{-\frac{1}{4l^2}\sum |z_i|^2}$. *Moore-Reed:* $\Phi^m(z_1, \ldots, z_n) = \prod_{i<j}(z_i - z_j)^m e^{-\frac{1}{4l^2}\sum |z_i|^2} Pf(\frac{1}{z_i - z_j})$. Energy spectrum of 2DEG breaks into allowed states $E_n = (n + \frac{1}{2})\hbar\omega_c$ in B field (Landau levels). When chemical potential lies in Landau bands, material is metallic. Otherwise localized states materialize adding electrons only add and subtract localized states, no currents flow and system is *incompressible. Magnetic length:* $l_B = \sqrt{\frac{\hbar}{eB}}$; within l_B of the edge, they form quasi-1D channels. Because there is no back-scattering, $R_{xx} = 0$. *Hidden subgroup:* $G^{abelian} \geq H$, $f : G \to X$ hides H if $f : G/H \leftrightarrow X$. *Filling factor:* Ratio of electrons to magnetic flux quanta. $\nu = \frac{1}{R_H}\frac{h}{e^2}$ or $\sigma_H = \nu\frac{e^2}{h}$. For composite fermions with p-filled Landau levels, $\nu = \frac{p}{2p+1}$. $\frac{1}{3}$ state is fully spin polarized. A *Luttinger liquid:* is composed of interacting electrons in a one dimensional conductor. The *Fermi energy* is the energy of the highest occupied quantum state in a system of fermions at absolute zero temperature.

Definitions: A *quantum dot* is a semiconductor whose excitons are confined in all three spatial dimensions. A *quantum well* is a semiconductor whose excitons are confined in two spatial dimensions. A *quantum wire* is a semiconductor whose excitons are confined in one spatial dimension. *Spin Polarization* is the degree to which the intrinsic angular momentum of elementary particles, is aligned with a given direction.

Some effects: The *Aharonov-Bohm* effect is a quantum mechanical phenomenon by which a charged particle is affected by electromagnetic fields in regions from which the particle is excluded. In the case of the Aharonov-Bohm solenoid effect, the wave function of a charged particle passing around a long solenoid experiences a phase shift as a result of the enclosed magnetic field, despite the magnetic field being zero in the region through which the particle passes. The *Coulomb blockade* is the increased resistance at small bias voltages of an electronic device comprising at least one low-capacitance tunnel junction. *Magnetic quantization:* $\Phi_0 = \frac{h}{2e} \approx 2 \times 10^{-15} Wb$; measured by Josephson effect. *Berry Phase:* Phase acquired in cyclic adiabatic process; measured through interference experiment. *Ising Model:* Spin coupling: $E = -\sum_{i,j} J_{ij} S_i S_j$. One dimensional: $E = \sum_i S_i S_{i+1}$. Two dimensional: $E = -\sum_{i,j} S_{i,j} S_{i,j+1} + S_{i,j} S_{i+1,j}$. Magnetic field breaks

the symmetry. Computational model: (1) Pick random site, (2) flip spin and calculate ΔE, (3) if $\Delta E < 0$, accept, (4) if $\Delta E > 0$ accept with probability $e^{-\beta \Delta E}$.

Aharonov-Bohm calculation for two slit experiment with small solenoid: $F = e(E + v \times B), E = -\nabla \times A - \frac{\partial A}{\partial t}, B = \nabla \times A$. Consider usual two slit set-up with electrons of wavelength λ, distance between slits d, second screen at distance L from first, a is leg of triangle with hypotheneuse d, and x is the distance from the center of the observation on the second screen. Without solenoid $\delta = \frac{2\pi a}{\lambda}$; if $x << L$, $\delta = \frac{x}{L}\frac{2\pi d}{\lambda}$. The field of the solenoid (in cylindrical coordinates) is $A_r = A_z = 0$ and $A_\phi = \frac{Br}{2}$ inside and $A_r = A_z = 0$ and $A_\phi = \frac{BR^2}{2r}$ outside where R is the radius of the solenoid. $B_z = \frac{1}{r}\frac{\partial A_\phi}{\partial r} - \frac{\partial A_r}{\partial \phi}$. Wave function of e^- is $\psi(p, r) = |\psi| exp(ip \cdot r) = |\psi| e^{i\alpha}$. The EM field changes $p \to p - eA$ so $\alpha \to \alpha - \frac{e}{\hbar} A \cdot r$. $\Delta\alpha = -\frac{e}{\hbar}\int_{path} A \cdot dr$ and thus $\Delta\delta = \Delta\alpha_1 - \Delta\alpha_2 = \frac{e}{\hbar}\int_{loop} A \cdot dr = \frac{e}{\hbar}\int_{loop} B \cdot dS = \frac{e}{\hbar}\Phi_B$.

Quantum computing: A *qubit* is a two dimensional space $|\psi >= a|0 > + b|1 >$ over $\mathbb{C}$ such that $|a|^2 + |b|^2 = 1$. A set of gates is said to be a set of *universal quantum gates* if any unitary operator can be approximated to arbitrary accuracy by a quantum circuit involving only those gates. The Hadamard, CNOT, phase and $\frac{\pi}{8}$ gates form a universal set. *A universal gate set:* $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$, $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $T = \begin{pmatrix} e^{-i\frac{\pi}{8}} & 0 \\ 0 & e^{i\frac{\pi}{8}} \end{pmatrix}$. *Pauli transformations:* $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$. $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_y = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$, $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Hamiltonian for EM: $H = \frac{1}{2m}(\vec{p} - \frac{q}{c}\vec{A}) \cdot (\vec{p} - \frac{q}{c}\vec{A}) + q\phi$. *Bennet's rules:* $X \geq Y$ means X can do the job of Y: (1) 1-qubit $\geq$ 1-bit, (2) 1-qubit $\geq$ 1-ebit, (3) 1-ebit +1-qubit $\geq$ 1-bit (dense coding), (4) 1-ebit +2-bits $\geq$ 1-qubit (teleportation).

$S^2|\alpha >= S(S+1)\hbar^2|\alpha >$, $S^2 = S_x^2 + S_y^2 + S_z^2$.

Projective measurements: $P_m = \sum_{i=1}^{m} |\phi_i\rangle\langle\phi_i|$. (1) State of system at $t = 0$ is ψ_0. (2) A measureable quantity, A, is described by an observable, A, acting on the state space. (3) Possible results are eigenvalues. (4) When A is measured, $P(a_n) = \sum_{i=1}^{g_n} |\langle u_n^i|\psi\rangle|^2$. (5) If the measurement of A in the state $|\psi\rangle$ gives a_n then immediately after the state is $\frac{1}{\sqrt{\langle\psi|P|\psi\rangle}} P_n|\psi\rangle$. $\langle A\rangle_\psi = \langle\psi|A|\psi\rangle$,

Quantum Ion Trap Systems: The qubits are representations of the hyperfine nuclear spin states at the lowest vibrational modes (phonons) of trapped atoms. Arbitrary transforms are constructed with laser pulses using Jaynes Cummings. Qubits interact via shared phonon state. Initial state preparation involves cooling atoms by trapping and optical pumping to their lowest motional ground and hyperfine state. The measurement is the measurement of the population of hyperfine states.

Spintronics: Spintronics exploits the intrinsic spin of electrons and their associated magnetic moment in solid-state devices. Electrons are spin-1/2 fermions and constitute a two-state system with spin "up" and spin "down".

Quantum error correcting conditions: Suppose C is a quantum code and P is a projection operator onto C. Suppose $\mathcal{E}$ is a quantum operator with measurements E_i. A necessary and sufficient condition for the existence of an error correction operator $\mathcal{R}$ is $PE_i^\dagger + E_j P = \alpha_{ij}$.

Non-abelian statistics: Let $R_1, R_2, \ldots, R_N$ be trajectories in $3+1$ dimensional space from t_i to t_f. $\psi(\vec{r_1}, \vec{r_2}) \rightarrow e^{i\theta}$. Normally, θ can either be 0 or π, if θ is arbitrary, this describes an *anyon*. Non-abelian anyons are associated with higher dimensional representations of the braid group. This can occur when there is a set of g degenerate states with particles are fixed $R_1, \ldots, R_N$. If $\{\psi_\alpha\}$ is an orthonormal basis and $\psi_\alpha \rightarrow [\rho(\sigma_1)]_{\alpha\beta}\psi_\beta$. It is non-abelian if $[\rho(\sigma_1)]_{\alpha\beta}[\rho(\sigma_2)]_{\beta\gamma} \neq [\rho(\sigma_2)]_{\alpha\beta}[\rho(\sigma_1)]_{\beta\gamma}$.

Cauchy-Schwartz: $\langle\phi|\psi\rangle \leq \langle\phi|\phi\rangle\langle\psi|\psi\rangle$. $T_{ij} = \langle u_i|T|u_j\rangle$ then $T = \sum_{ij} T_{ij}|u_i\rangle\langle u_j|$. *Continuous version of inner product:* $\langle\phi|\psi\rangle = \int \phi^*\psi dx$. If $|\phi\rangle = \sum_i c_i|u_i\rangle$ then $\psi\rangle \rightarrow \begin{pmatrix} c_1 \\ c_2 \\ \ldots \\ c_n \end{pmatrix} = \begin{pmatrix} \langle u_1|\psi\rangle \\ \langle u_2|\psi\rangle \\ \ldots \\ \langle u_n|\psi\rangle \end{pmatrix}$. If $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ then $|\langle 0|\psi\rangle|^2 = |\alpha|^2$. *Projection operator:* $P_m = \sum_{i=1}^m |u_i\rangle\langle u_i|$. *Observables:* Hermitian operators on state vectors. Observables A, B commute iff there is a basis of eigenvalues that commute.

$|\psi(t)\rangle = (\alpha(t), \beta(t))^T$. $H|\psi\rangle = \begin{pmatrix} \omega_1 & \omega_2 \\ \omega_2 & \omega_1 \end{pmatrix}\begin{pmatrix} \alpha(t) \\ \beta(t) \end{pmatrix} = i\hbar\frac{\partial|\psi\rangle}{\partial t} = \begin{pmatrix} \frac{d\alpha(t)}{dt} \\ \frac{d\beta(t)}{dt} \end{pmatrix}$, $\alpha(t) = e^{i\frac{\omega_1 t}{\hbar}} cos(i\frac{\omega_2 t}{\hbar}))$.

$\langle w|T^\dagger|v\rangle = \langle v|T|w\rangle^*$, $[X, P] = i\hbar$. Finding similarity: (1) find eigenvalues/eigenvectors, (2) normalize eigenvectors, v_i, (3) $S^{-1} = (v_1, \ldots, v_n)$.

Hadamard Gate: $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. **Pauli matricies:** $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. $\vec{L} = \vec{r} \times \vec{p}$, $L_x = yp_z - zp_y$, $[L_x, L_y] = i\hbar L_z$. $(\Delta A)^2(\Delta B)^2 \geq (\frac{\langle A,B\rangle}{2i})^2$.

Degeneracy (duplicate eigenvalues): Suppose A has g_m degenerate states then $Prob(\lambda_m) = \sum_{i=1}^{g_m} |\langle a_m^i|\psi\rangle|^2$.

Tensor: $\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$.

Density Operator: $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$. If system is in a pure stare $Tr(\rho) = 1$; if system is in a mixed state $Tr(\rho) < 1$.

Spin: Bosons: $swap(|AB\rangle) = |BA\rangle$, if 2 bosons are distributed in 3 boxes, the probability two are in the same box is $\frac{1}{2}$. Fermions: $swap(|AB\rangle) = -|BA\rangle$, if 2 fermions are distributed in 3 boxes, the probability two are in the same box is $\frac{1}{3}$. Feynman's QED: $P(A \rightarrow B) = \sum_{\gamma_i} |A_{A\rightarrow B}^{\gamma_i}|^2$ where the $\{\gamma_i\}$ are the paths from $A \rightarrow B$.

Ladder operators: Remember $-\frac{\hbar^2}{2m}\frac{\partial^2\Psi(x,t)}{\partial x^2} + U\Psi(x,t) = i\hbar\Psi(x,t)$, $\int|\Psi|^2 = 1$. Define $a_\pm = \frac{1}{\sqrt{2m}}(\frac{\hbar}{i}\frac{\partial}{\partial x} \pm i\omega x)$, $[a_+, a_-] = \hbar\omega$. $\Psi_{EPR} = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$.

Mach-Zender interferometer: Input state is $|U\rangle$. Along upper path state is $\frac{1}{\sqrt{2}}(|U\rangle + |L\rangle)$. Along lower path state is $\frac{1}{\sqrt{2}}(|U\rangle - |L\rangle)$. At detector 1, state is $\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}[(|U\rangle + |L\rangle) + (|U\rangle - |L\rangle)] = |U\rangle$. At detector 0, state is 0.

Bell's Argument against hidden variables: Consider two entangled total spin zero particles parti-

cles #1, #2, A and B are measurements on #1. C and D are measurements on #2. $\Psi = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$. EPR argument is that entanglement and locality mean hidden variables. Assuming locality, any measurement on #1 does not effect C or D measurements. If $P(A = C) = P(B = D) = 0.85$ and $P(B = C) = 1$ then $P(A = D) \geq .7$. Prepare axis so that (1) the angle between A and C is 135, (2) the angle between B and C is 180, (3) the angle between B and D is 135, (4) the angle between A and D is 45. Quantum mechanics gives $P(A = C) == P(B = C) = .85$ and $P(B = C) = 1$ but $P(A = D) = .5 < .7$. Thus entanglement, locality and quantum mechanics are inconsistent. Locality loses.

The braid calculation: $|\Psi_1\rangle = U(t)|\Psi_0\rangle$; a phase error θ is introduced when $a|0\rangle + b|1\rangle \rightarrow a|0\rangle + be^{i\theta}|1\rangle$. A system has a topological phase if its low energy, long distance effective field theory is a topological field theory, that is, physical correlations are topologically invariant up to a correlation of order $e^{\Delta/T}$. *Anyon*: Any phase factor $e^{\imath\phi}$ can result from a counter-clockwise exchange of two particles. Feynman: Paths are weighted by $e^{iS/\hbar}$, S is classical action. Suppose there are g degenerate states Ψ_a, $a = 1, 2, \ldots, `g$ of particles at positions $x_1, x_2, \ldots, x_n$. Exchange rotates states according to (say) $\Psi_a \rightarrow M_{ab}\Psi_b$ for $1, 2$ exchange and $\Psi_a \rightarrow N_{ab}\Psi_b$ for $2, 3$ exchange. Exchange statistics are *non-abelian* if $M_{ab}N_{ab} \neq N_{ab}M_{ab}$. We can read the state by using the non-abelian A-B effect: Send a non-abelian anyon test quasi-particle around hall bar edge, interference effect determines state. $\sigma_{xx} \propto |t_1 + it_2|^2$

Symmetries: EM ($U(2)$), Weak ($SU(2)$), Strong ($SU(3)$). A *Lie group* (1) depends on parameters $\theta_1, \ldots, \theta_n$ and (2) derivatives with respect to group parameters exist. The diffeomorphism group of a Lie group acts transitively on the Lie group. $g(\theta)_{\theta=0} = e$, $\frac{\partial g(\theta_1,\ldots,\theta_n)}{\partial\theta_i}_{\theta_j=0} = iX_j$ are the generators. $[X_i, X_j] = if_{ijk}X_k$ is group algebra. Consider $R_x(\zeta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & cos(\zeta) & sin(\zeta) \\ 0 & -sin(\zeta) & cos(\zeta) \end{pmatrix}$, $R_y(\phi) = \begin{pmatrix} cos(\phi) & 0 & sin(\phi) \\ 0 & 1 & 0 \\ -sin(\phi) & 0 & cos(\phi) \end{pmatrix}$, and $R_z(\theta) = \begin{pmatrix} cos(\theta) & sin(\theta) & 0 \\ -sin(\theta) & cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Unitary: $[U, H] = 0$. $SU(2)$ has 3 generators and $SU(3)$ has 8.

Noether: If $T(s)$ is a transformation $T(s) : q \mapsto q(s)$ and $\frac{\partial L(q(s)}{\dot{q}(s)} = 0$, then $C = p\frac{\partial q(s)}{\partial s}$ is a conserved quantity.

Model for electron flow in crystal: Let C_n be the wave function at site n in a linear array of molecules in a lattice each separated by a distance b. $i\hbar\frac{\partial C_{n-1}}{\partial t} = E_0C_{n-1} - AC_n - AC_{n-2}$. $C_n = a_n(x)e^{-i(e/\hbar)t}$ and $a_n(x) = e^{ikx}$. Substituting,$E = E_0 + A(e^{-ikx} + e^{ikx})$. Using $E_0 = 2A$ and $cos(t) \approx 1 - t^2/2$ for small t, we get $E = \hbar\omega = \frac{Ab^2k^2}{2}$ so $\frac{d\omega}{dk} = \frac{2Ab^2}{\hbar}k$. If E is different, say $E_0 + F$ at site 0, we get backscattering or trapping depending on the sign of F.

Semiconductor junctions: $\frac{N_p(p-side)}{N_p(n-side)} = e^{-\frac{q_pV}{kT}}$. The energy in conduction band $\approx E_0 + \alpha k^2$. $N_nN_p = ce^{E_{gap}/(kT)}$. $E_{gap,Ger} \approx .72ev$, $E_{gap,Si} \approx 1.1ev$; at room temperature, $kT \approx \frac{1}{40}ev$. $v_{drift} = \frac{q_n\mathcal{E}\tau_n}{m_n}$, yielding the Ohm law: $\vec{j} = \frac{Nq_n^2\tau_n}{m_n}\vec{\mathcal{E}}$. For Hall effect, $\vec{E_{tr}} = -\vec{v}_{drift} \times \vec{B} = -\frac{1}{qN}B\vec{j}$, $R_H = \frac{1}{qN}$.

4.6 Background for Quantum Field Theory

Compton Scattering: Photon of wavelength λ scatters off stationary electron of mass m resulting in photon of wavelength λ' at an angle θ and m acquiring momentum p. $\lambda' = \lambda + \frac{h}{mc}(1 - cos(\theta))$.

Spin: It is impossible to measure all components of $L = (L_x, L_y, L_z)$ simultaneously. We can measure L^2 and

L_z simultaneously. $L^2|\psi\rangle = \hbar^2 l(l+1)|\psi\rangle$ and $L_z|\psi\rangle = \hbar m_l|\psi\rangle$, $-l \le m_l \le l$ ($2l$+1-dimensional Hilbert space). Same for spin; namely, $S^2|\psi\rangle = \hbar^2 s(s+1)|\psi\rangle$ and $S_z|\psi\rangle = \hbar m_s|\psi\rangle$, $-s \le m_s \le s$. The states are sometimes denoted $|l, m_l\rangle$ and $|s, m_s\rangle$ respectively. *Clebsh-Gordon*: $|j_1, m_1\rangle|j_2, m_2\rangle = \sum_j C^{j,j_1,j_2}_{m,m_1,m_2}|j, m\rangle$. Orbital state $|3, -1\rangle$, spin state $|\frac{1}{2}, \frac{1}{2}\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|\frac{1}{2}, -\frac{1}{2}\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. $\hat{S}_x = \frac{\hbar}{2}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\hat{S}_y = \frac{\hbar}{2}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ and $\hat{S}_z = \frac{\hbar}{2}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The $\chi_t = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \pm\frac{1}{\sqrt{2}} \end{pmatrix}$. For spinor, $\begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = U(\theta)\begin{pmatrix} \alpha \\ \beta \end{pmatrix} =$, $U(\theta) = e^{i(\theta\cdot\sigma)/2}$.

Parity, charge conjugation and time reversal: TCP Theorem.

Bound states: e^-, p^+ (hydrogen), e^+, e^- (positronium), $c, \bar{c}$ (charmonium). Central force, $\psi(r, \theta, \phi) = \frac{u(r)}{r}Y_l^{m_l}(\theta, \phi)$ where $u(r)$ satisfies $-\frac{\hbar^2}{2m}\frac{d^2}{dr^2} + [V(r)\frac{\hbar^2}{2m}\frac{l(l+1)}{r^2}]u = Eu$.

Calculating decay and scattering with Feynman diagrams: *Lifetime* is denoted by Γ and $dN = \Gamma N dt$. Each branching has lifetime Γ_i and $\Gamma_{tot} = \sum_i \Gamma_i$. *Cross section* is denoted σ and $\sigma_{tot} = \sum_i \sigma_i$. Scattering angle depends on the impact parameter, b. For hard scattering on a sphere of radius, R, $b = Rsin(\alpha), 2\alpha + \theta = 2\pi$, $b = Rcos(\frac{\theta}{2})$. $\frac{db}{d\theta} = -\frac{R}{2}sin(\frac{\theta}{2})$. $\sigma = \int \frac{R^2}{4}d\Omega$. To calculate Γ_i, σ_i, we neet the amplitude $\mathcal{M}$ and apply the "golden rule" in phase space. For $1 \to 2 + 3 + \ldots + n$, the golden rule is $\Gamma = \frac{S}{2\hbar m_1}\int \mathcal{M}^2(2\pi)^4\delta(p_1 - p_2 - p_3 - \ldots - p_n) \times \prod_{j=2}^n 2\pi\delta(p_j^2 - m_2^2c^2)\theta(p_j^{(0)})\frac{d^4p_j}{(2\pi)^4}$. For Feynman diagram, (1) label incoming edges and outgoing edges with four vectors $p_1, \ldots, p_n$ and note direction, label internal edges with $q_1, \ldots, q_m$,(2) for each vertex label coupling constant (e.g.- ig), (3) get propagators for internal edges by writing factor $\frac{i}{q_j^2 - m_j^2c^2}$, (4) for each vertex write δ function (e.g. - $\delta(k_1 + k_2 + k_3)$, + for out edges, − for in edges (Kirchoff applies), (5) for each internal edge, write $\frac{1}{(2\pi)^4}d^4q_i$ and (5) cancel the deltas and nultiply by $\mathcal{M}$. For example, $\Gamma = \frac{g^2|p|}{8\pi\hbar m_A c}$, $p = \frac{c}{2m_A}(\sqrt{m_A^4 + m_B^4 + m_C^4 - 2m_A^2m_B^2 - 2m_B^2m_C^2 - 2m_A^2m_C^2})$.

Quasi-particles and Fermions: Quasi-particles are composite particles. One analogy is a positive ion with a retinue of negative ions. A simple example is two masses, m_1, m_2 connected by a strong spring. One quasi-particle is the center of mass, the second the reduced mass system $\frac{m_1m_2}{m_1+m_2}$. The highest filled particle level of a collection of fermions in the ground state is the *Fermi level*, ϵ_F with momentum $k_F = \sqrt{2m\epsilon_F}$. The energy sphere filled by the particles is called the *Fermi sea* and the surface of the sphere is the *Fermi surface*. A total single particle propagator is the sum of the amplitudes for all possible ways a particle can propagate through a system.

Three pictures of quantum mechanics: The *Schroedinger picture* gives $i\hbar\frac{d}{dt}|A, t\rangle_S = H|A, t\rangle_S$; solve for $|A, t_0\rangle$ evolve via $|A, t\rangle = U|A, t_0\rangle_S$, $U = e^{iH(t-t_0)/\hbar}$. In the *Heisenberg model*, $|A, t\rangle_H = U^\dagger|A, t\rangle_S$; time dependance is captured by the operator $O^H(t) = U^T O^S U$ and $[O^S, P^s] = C = [O^H(t), P^H(t)]$ while $i\hbar\frac{d}{dt}O^H(t) = [O^H(t), H]$. For the *interaction picture*, $H = H_0 + H_I$ where H_0 describes the independent fields and H_I describes the interaction of the fields. Here, $U_0(t, t_0) = e^{-iH_0(t-t_0)/\hbar}$, $|A, t\rangle_I = U_0^\dagger|A, t\rangle_S$ and $O^I(t) = U_0^\dagger O^S U_0$.

Classical radiation: $\nabla \cdot A = 0$, $A(x, t) = A_0 e^{i(k\cdot x - \omega t)}$ and $k \cdot A = 0$. $H_{rad} = \frac{1}{2}\int E^2 + B^2\, d^3x$. For periodic boundary $A(0, y, z, t) = A(L, y, z, t)$, $\frac{a}{\sqrt{V}}\epsilon_r(K)e^{ik\cdot x}$ is a complete set of fields and $k = \frac{2\pi}{L}(n_1, n_2, n_3)$. $\epsilon_r(k) \cdot \epsilon_s(k) = \delta_{rs}$ and $\epsilon_r(k)\cdot k = 0$. The vector potential can be written as $A(x, t) = \sum_k \sum_r (\frac{\hbar c^2}{2V\omega_k})^{1/2}\epsilon_r(k)[a_r(k, t)e^{ik\cdot x} + a_r^*(k)e^{-ik\cdot x}]$ where $\omega_k = c|k|$. Substituting into $\Box A = 0$ gives $\frac{\partial a_r(k,t)}{\partial t} = -\omega_k^2 a_r(k, t)$ and we set $a_r(k, t) = a_r(k)e^{-1\omega_k t}$ and $H_{rad} = \sum_k \sum_r \hbar\omega_k a_r^*(k)a_r(k)$.

Harmonic Oscillator: $H_{osc} = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 q^2$ with $[p,q] = i\hbar$. put $a = (\frac{1}{2\hbar m\omega})^{1/2}(m\omega q + ip)$ and $a^\dagger = (\frac{1}{2\hbar m\omega})^{1/2}(m\omega q - ip)$ with $[a, a^\dagger] = 1$. $H_{osc} = \hbar\omega(a^\dagger a + \frac{1}{2})$ and we put $N = a^\dagger a$. Note that $\langle\Phi|N|\Phi\rangle = \langle a\Phi|a\Phi\rangle \geq 0$ and the lowest eigenvalue of N is 0. Further $Na|\alpha\rangle = (\alpha - 1)a|\alpha\rangle$ and $Na^\dagger|\alpha\rangle = (\alpha + 1)a^\dagger|\alpha\rangle$ while $|n\rangle = \frac{(a^\dagger)^n}{\sqrt{n!}}|0\rangle$. These are eigenvalues of H_{osc} so $E_n = \hbar\omega(n + \frac{1}{2})$. Finally, since $i\hbar\frac{da(t)}{dt} = [a(t), H_{osc}]$, $a(t) = ae^{-i\omega t}$.

Quantized radiation field: $[a_r(k), a_s^\dagger(k')] = \delta_{rs}\delta_{kk'}$ and $[a_r(k), a_s(k')] = [a_r^\dagger(k), a_s^\dagger(k')] = 0$ so $H_{rad} = \sum_r\sum_k \hbar\omega[a_r(k)^\dagger a_r(k) + \frac{1}{2}]$. $N_r(k) = a_r(k)^\dagger a_r(k)$ have eigenvalues $0, 1, 2, \ldots$ and eigenfunctions $|n_r(k)\rangle = \frac{(a_r^\dagger)^{n_r(k)}}{\sqrt{n_r(k)}}|0\rangle$. $P = \sum_k\sum_r \hbar k(N_r(k) + \frac{1}{2})$. The lowest energy state has all 0 occupancy numbers and $E_0 = \frac{1}{2}\int d^k\hbar\omega_k$ which is *infinite* and must be removed. In the Heisenberg picture, we write $A(x,t) = A(x,t)^+ + A(x,t)^-$ with $A(x,t)^+ = \sum_k\sum_r(\frac{\hbar c^2}{1V\omega_k})^{1/2}\epsilon_r(k)a_r(k)e^{i(k\cdot x - \omega_k t)}$ (the absorption operators) and $A(x,t)^- = \sum_k\sum_r(\frac{\hbar c^2}{1V\omega_k})^{1/2}\epsilon_r(k)a_r^\dagger(k)e^{-i(k\cdot x - \omega_k t)}$ (the emission operators). Since $[H, a_r(k)] = [H, a_r^\dagger(k')] = 0$, the $n_r(k)$ are constants.

Interaction with dipole field: Suppose $H_I = -D\cdot E_T(0,t)$ where $D = \sum_i e_i r_i$, generally we can ignore the magnetic dipoles. For intial state A and final state B, we have $|A, n_r(k)\rangle = |A\rangle|n_r(k)\rangle$ and $|B, n_r(k) \pm 1\rangle = |B\rangle|n_r(k) \pm 1\rangle$ and $E_T(0,t) = i\sum_k\sum_r(\frac{\hbar\omega_k}{2V})^{1/2}\epsilon_r(k)[a_r(k)e^{-i\omega_k t}a_r^\dagger(k)e^{i\omega_k t}]$. For emission, $\langle B, n_r(k) + 1|H_I|A, n_r(k)\rangle = i(\frac{\hbar\omega_k}{2V})^{1/2}\langle n_r(k)+1|a_r^\dagger|n_r(k)\rangle\langle B|\epsilon_r(k)\cdot D|A\rangle e^{i\omega_k t} = i(\frac{\hbar\omega_k}{2V})^{1/2}\langle\sqrt{n_r(k)+1}\langle B|\epsilon_r(k)\cdot D|A\rangle e^{i\omega_k t}$. The transition probability between initial and final states per unit time can be solved with perturbation theory to give $w = \frac{2\pi}{\hbar}|\langle B, n_r(k) + 1|H_I|A, n_r(k)\rangle|^2\delta(E_A - E_B - \hbar\omega_k)$. So $w_{tot}(A \to B) = \frac{e^2\omega^3}{3\pi\hbar c^3}|x_{BA}|^2$ and the lifetime τ of the excited state is $\frac{1}{\tau} = \sum_n w_{tot}(A \to B_n)$. The total angular momentum and its z-component, J and M must satisfy the selection rule $\Delta J, \Delta M = (0, \pm 1)$.

Order parameters: Water is more symmetric than ice on average. Transition to ice is a *broken symmetry*. The order parameter is related to bond formation. For magnets, the order parameter is a sphere representing orientation. For a crystal with periodic structure, it is the distance from a reference atoms and the space is a square with identified edges, i.e.- a torus. In He^4, it is the condensate wave function. Superfluids have broken gauge symmetries.

4.7 Quantum Field Theory

Reminder: To find extrema functional $x(t)$, solve $\delta \int_{t_1}^{t_2} L(x,\dot{x})dt = 0$ by solving $\frac{\partial L}{\partial x} - \frac{d}{dt}(\frac{\partial L}{\partial \dot{x}}) = 0$. $L = T - V$, $H = \sum_i p_i \dot{q}_i - L$, $p_i = \frac{\partial L}{\partial \dot{q}_i}$. Canonical quantization replaces scalars with operators (e.g. - p, etc).

Infinite degrees of freedom: Quantum Field Theory describes quantum systems with an infinite number of degrees of freedom. Here is an example: Consider n particles of mass m connected by identical springs with spring constant k. Let y_i be the displacement of the particles from their equilibrium position. $L = \frac{1}{2}\sum_{i=1}^{n}[m\dot{y_i} - k(y_{i+1} - y_i)^2] = \frac{1}{2}\sum_{i=1}^{n} a[\frac{m}{a}\dot{y_i} - k\frac{(y_{i+1}-y_i)^2}{a}] = a\sum_{i=1}^{n} L_i$. Let $n \to \infty$ then $\frac{m}{a} \to \mu$, the linear density, $\frac{y_{i+1}-y_i}{a} = \frac{\partial y}{\partial x}$ and $ka = Y$. $\delta \int_{t_1}^{t_2} dt \int_{x_0}^{x_1} dx(\frac{1}{2}[\mu\dot{y}^2 - Y(\frac{\partial y}{\partial x})^2]) = 0$ gives $\frac{\partial}{\partial x}\frac{\partial \mathcal{L}}{\partial \frac{\partial y}{\partial x}} + \frac{\partial}{\partial t}\frac{\partial \mathcal{L}}{\partial \frac{\partial y}{\partial t}} - \frac{\partial \mathcal{L}}{\partial y}$; where the term in the second integral is called the Lagrangian density denoted $\mathcal{L}$. The corresponding Hamiltonian density is $\mathcal{H} = \dot{y}\frac{\partial \mathcal{L}}{\partial \dot{y}} - \mathcal{L}$.

Maxwell's equations as four vectors: $b_\mu = (\vec{b}, ib_0)$; Lorentz transform is $x'_\mu = a_{\mu,\nu}x_\nu$ and $\partial'_\mu F = \partial'_\mu(x_\nu)\partial_\nu(F)$. Let j_μ be the four-vector $j_\mu = (\vec{j}, ic\rho)$ and

$$F_{\mu,\nu} = \begin{pmatrix} 0 & B_3 & -B_2 & -iE_1 \\ -B_3 & 0 & B_1 & -iE_2 \\ B_2 & -B_1 & 0 & -iE_3 \\ iE_1 & iE_2 & iE_3 & 0 \end{pmatrix}.$$

Maxwell's equations become $\frac{\partial F_{\mu\nu}}{\partial x_\nu} = \frac{j_\mu}{c}$. Note the matrix is anti-symmetric. This is also written as $\partial_\nu F_{\mu\nu} = \frac{j_\mu}{c}$. $F_{\mu\nu}F_{\mu\nu} = 2(|B|^2 - |E|^2)$ is a scalar. $F_{uv} = \partial_u A_v - \partial_v A_u$. Klein Gordon in four vector format: $\mathcal{L} = \frac{1}{2}\eta^{uv}\partial_u\partial_v\phi - \frac{1}{2}m\phi^2$ where $\eta_{uv} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$; this is Minkowski's metric. A tensor, v_i is *covariant* if it transforms as $(v_i)' = \frac{\partial x_j}{\partial x_i}v_j$. A tensor, v^i is *contravariant* if it transforms as $(v^i)' = \frac{\partial x^i}{\partial x^j}v^j$. Differentials are contravariant, ∇ is covariant.

Lorentz rotation by θ followed by boost of v along x is

$$\begin{pmatrix} \gamma & -\gamma v & 0 & 0 \\ -\gamma v & \gamma & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & cos(\theta) & -sin(\theta) & 0 \\ 0 & sin(\theta) & cos(\theta) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \gamma = \frac{1}{\sqrt{1 - v^2/c^2)}}.$$

Yukawa potential: Neutral scalar field, $\mathcal{L} = -(\frac{1}{2}(\frac{\partial \phi}{\partial x_\mu})^2 + \mu^2\phi^2)$. $E^2 - |p|^2c^2 = m^2c^4$. $E \to i\hbar\frac{\partial}{\partial t}$ and $p \to -i\hbar\frac{\partial}{\partial x_\mu}$, $\mu \leftrightarrow \frac{mc}{\hbar}$. Use the usual Fourier correspondance $\tilde{\phi}(k) = \frac{1}{(2\pi)^{3/2}}\int d^3x(e^{-k\cdot x}\phi(x))$ and $\phi(x) = \frac{1}{(2\pi)^{3/2}}\int d^3k(e^{k\cdot x}\tilde{\phi}(k))$. Now consider a scalar potential field, ϕ, with a point source, G, satisfying the Klein-Gordon equation $\Box^2\phi = G\delta^{(3)}(x)$. Multiply both sides by $\frac{1}{(2\pi)^{3/2}}(e^{-ik\cdot x})$ and integrate remembering that ϕ and its derivatives vanish at the limits of integration. We get $(-|k|^2 - \mu^2)\tilde{\phi}(k) = G\frac{1}{(2\pi)^{3/2}}$, so $\phi(x) = \frac{e^{-\mu r}}{r}$ and $\mathcal{H}_{int} = -\mathcal{L}_{int}$.

Transformations: $\begin{pmatrix} \phi_1' \\ \phi_2' \end{pmatrix} = \begin{pmatrix} cos(\lambda) & -sin(\lambda) \\ sin(\lambda) & cos(\lambda) \end{pmatrix} \begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix}$ for free fields of identical mass. Consider n scalar fields ϕ_a with the same mass and $\mathcal{L}$. $\mathcal{L} = \frac{1}{2}\sum_{i=1}^{n} \partial_\mu \phi_a \partial_\mu \phi_a - \frac{1}{2}\sum_{i=1}^{n} m^2 \phi_a^2 - g(\sum_{i=1}^{n} \phi_a^2)^2$, $\mathcal{L}$ is invariant under $G = SO_n$. Non-abelian symmetries are global symmetries. Translation invariance gives *conservation of momentum.* Time invariance gives *conservation of energy. First quantization* promotes values (position, momentum, energy) to operators ($E \to i\hbar\frac{\partial}{\partial t}$, $p \to -i\hbar\nabla$) and impose commutator realtionships. *Second quantization* position, momentum, energy etc. remain scalar but fields like potential and conjugate momentum become operators; commutator relations imposed on field operators.

Invariance and conserved quantities: If $i\hbar\frac{dO(t)}{dt} = [O(t), H] = 0$, O is a constant of the motion. Now let $|\Phi\rangle \to |\Phi'\rangle = U|\Phi\rangle$ so $O = U^\dagger O U$; often $U = e^{i\alpha T}$ where α is a continuous parameter. For an infinitesimal translation, $U = I + i\delta\alpha T$ and $\delta O = i\delta\alpha[T, O]$. Invariance of the Lagrangian under a transformation, leads to $\frac{\partial f^\alpha}{\partial x^\alpha} = 0$ and $F^\alpha(t) = \int d^3x \frac{\partial f^\alpha}{\partial x^\alpha}$ is a conserved quantity. For example, suppose $\phi_r(x) \to \phi_r'(x) = \phi_r(x) + \delta\phi_r(x)$. The Lagrangian transforms as $\delta(\mathcal{L}) = \frac{\partial \mathcal{L}}{\partial \phi_r}\delta\phi_r + \frac{\partial \mathcal{L}}{\partial \phi_{r,\alpha}}\delta\phi_{r,\alpha}$ which applying the minimum condition becomes $\delta(\mathcal{L}) = \frac{\partial}{\partial x^\alpha}\frac{\partial \mathcal{L}}{\partial \phi_{r,\alpha}}\delta\phi$; here, $f^\alpha = \frac{\partial \mathcal{L}}{\partial \phi_{r,\alpha}}\delta\phi$. This gives $Q = \frac{-iq}{\hbar}\int d^3x[\pi_r(x)\phi_r(x) - \pi^\dagger\phi^\dagger]$ as a conserved quantity. Q is charge. If instead we consider translation invariance we get conservation of energy/momentum. Rotational invariance gives conservation of angular momentum.

Standard script for classical $\to$ quantum field theory: Promote conjugate variables to operators $\langle\phi_r, \pi_s\rangle$ and *quantize* as $[\phi_r(j,t), \pi_s(j',t)] = i\hbar\delta_{rs}\delta_{jj'}$, $[\phi_r(j,t), \phi_s(j',t)] = [\pi_r(j,t), \pi_s(j',t)] = 0$, and $[\phi_r(x,t), \pi_s(x',t)] = i\hbar\delta_{rs}\delta(x - x')$.

The complex potential: Consider two real scalar fields ϕ_1, ϕ_2 and put $\phi = \frac{1}{\sqrt{2}}(\phi_1 + i\phi_2)$. If ϕ is the solution to the Klein Gordon equation in the presence of a potential A_μ with charge e, then ϕ^* is the solution to the Klein Gordon equation in the presence of a potential A_μ with charge $-e$. The *charge current density,* $s_\mu = i(\frac{\partial\phi^*}{\partial x_\mu}\phi - \phi^*\frac{\partial\phi}{\partial x_\mu})$ satisfies $\frac{\partial s_\mu}{\partial x_\mu} = 0$.

Creation and annihilation operators: We look at photons. Let $\mu_{k,\alpha}(x) = \epsilon^{(\alpha)}(k)e^{ik\cdot x}$ where α is the linear polarization selected so that $\epsilon^{(1)}, \epsilon^{(2)}, k$ form an oriented orthogonal triad. Consider the potential bounded in space by a cube of side length L, $V = L^3$. $A(x,t) = \frac{1}{V^{1/3}}\sum_k \sum_{\alpha=1,2}(c_{k,\alpha}\mu_{k,\alpha}(x) + c_{k,\alpha}^*\mu_{k,\alpha}^*(x))$. We have $H = \frac{1}{2}\int(|B|^2 + |E|^2)d^3x$, $H = \sum_k \sum_\alpha 2(\frac{\omega}{c})^2 c_{k,\alpha}^* c_{k,\alpha}$. Put $Q_{k,\alpha} = \frac{1}{c}(c_{k,\alpha} + c_{k,\alpha}^*)$, and $P_{k,\alpha} = -\frac{\omega}{c}(c_{k,\alpha} - c_{k,\alpha}^*)$. $\frac{\partial H}{\partial Q_{k,\alpha}} = -\dot{P}_{k,\alpha}$ and $\frac{\partial H}{\partial P_{k,\alpha}} = \dot{Q}_{k,\alpha}$, We get $\frac{1}{V^{1/3}}\int d^3x(\mu_{k,\alpha}\cdot\mu_{k',\alpha'}^*) = \delta_{k,k'}\delta_{\alpha.\alpha'}$, $k_x, k_y, k_z = \frac{2\pi n}{L}$ and $\omega = |k|c$. Make $P_{k,\alpha}$ and $Q_{k,\alpha}$ operators as usual giving $[Q_{k,\alpha}, P_{k',\alpha'}] = \pm i\hbar\delta_{k,k'}\delta_{\alpha,\alpha'}$, $[Q_{k,\alpha}, Q_{k',\alpha'}] = 0$, $[P_{k,\alpha}, P_{k',\alpha'}] = 0$. The *annihilation operator* is $a_{k,\alpha} = \frac{1}{\sqrt{2\hbar\omega}}(\omega Q_{k,\alpha} + iP_{k,\alpha})$. The *creation operator* is $a_{k,\alpha}^\dagger = \frac{1}{\sqrt{2\hbar\omega}}(\omega Q_{k,\alpha} - iP_{k,\alpha})$. $N_{k,\alpha} = a_{k,\alpha}^\dagger a_{k,\alpha}$. $N|n\rangle = n|n\rangle$, $Na^\dagger|n\rangle = (n+1)|n\rangle$, $Na|n\rangle = (n-1)|n\rangle$.

Aharonov Bohm: For double slit setup with puddle of $B \neq 0$ completely inside the strip of the two slits. $\phi = \phi_1^{(0)} exp[\frac{ie}{\hbar c}\int_{path1} A(x')\cdot dx'] + \phi_2^{(0)} exp[\frac{ie}{\hbar c}\int_{path2} A(x')\cdot dx']$. $\int_{closed\ path} A(x')\cdot dx' = \int_{surface} B\cdot n\ dS = \frac{e\Phi}{\hbar c}$. For superconducting ring, with Cooper pair quasi-particle, $\phi = \phi^{(0)} exp[\frac{2ie}{\hbar c}\int_{closed\ path} A(x')\cdot dx']$. Since ϕ is the same whether or not the path encloses the flux; $\frac{2e}{\hbar c}\int_{closed\ path} A(x')\cdot dx' = 2n\pi$, so $\Phi = \frac{n\pi\hbar c}{e}$.

Pauli matricies and the Dirac equation: $\sigma_1 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\sigma_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Particle	Mass	Particle	Mass
1	2	...	n
Neutrino	$10^{-2}eV$	Proton/Neutron	$1GeV$
Electron	$.5MeV$	τ	$2GeV$
Muon	$100MeV$	W, Z Boson	$80-90GeV$
Pion	$140MeV$	W, Z Higgs	$120-200GeV$

Particles from the vacuum: $[H, a_p^\dagger] = \omega_p a_p^\dagger$, $[H, a_p] = -\omega_p a_p$, $|p\rangle = a_p^\dagger|0\rangle$ and $H|p\rangle = \omega_p|p\rangle$, $\omega_p^2 = p^2 + m^2$. $P|p\rangle = p|p\rangle$.

The Dirac equation: $(i\gamma^u\partial_u - \frac{mc}{\hbar})\phi = 0$. Time reversal transformation is $T : x^0 \to -x^0$; $x^i \to x^i$. Parity reversal transformation is $P : x^0 \to x^0$; $x^i \to -x^i$. $\gamma_k = \begin{pmatrix} 0 & -i\sigma_k \\ i\sigma_k & 0 \end{pmatrix}$, $\gamma_0 = \begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}$. Dirac wanted to find a field equation with linear operators: $E = \alpha \cdot p + \beta m$, $i\frac{\partial\phi}{\partial t}(-i\alpha \cdot \nabla + \beta m)\phi$ and require $E^2 = m^2 + |p|^2$. $\alpha = \begin{pmatrix} 0 & \sigma \\ \sigma & 0 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Under spacetime transformation, spinor transforms as $\delta\phi = \epsilon^u\partial_u\phi$. $T^{\mu\nu}\partial^\mu\phi\partial^\nu\phi - \eta^{\mu,\nu}\mathcal{L}$.

Angular momentum: $L = r \times p$. If $[H, L] = 0$, angular momentum is conserved. $[H, L] = [\alpha \cdot p, r \times p] = i\alpha \times p$. $\Sigma = \begin{pmatrix} \sigma & 0 \\ 0 & \sigma \end{pmatrix}$, $[H, \Sigma] = [\alpha \cdot p, -i\alpha_1\alpha_2\alpha_3\alpha] = 2i\alpha \times p$. $J = L + \frac{1}{2}\Sigma$ is conserved, $[H, J] = 0$. Lagrangian for free Dirac field is $\mathcal{L} = \overline{\phi}(i\gamma^u\partial_u - m)\phi = \phi_i(i[\gamma^u]_{ij}\partial_u - m\delta_{ij})\phi_j$.

Solving the Dirac equation for a free scalar field: $(i\gamma^0\partial_t - m)\phi = 0$, gives $i\gamma^0\partial_t\phi = i\begin{pmatrix} I & 0 \\ 0 & -I \end{pmatrix}$ or $\begin{pmatrix} \frac{\partial u}{\partial t} \\ \frac{\partial u}{\partial t} \end{pmatrix} = m\begin{pmatrix} u \\ v \end{pmatrix}$, where $u = \begin{pmatrix} \phi_1 \\ \phi_2 \end{pmatrix}$ and $u = \begin{pmatrix} \phi_3 \\ \phi_4 \end{pmatrix}$. Note u and v correspond to spin states; $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ is spin up and $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ is spin down. Thus $i\dot{u} = mu$ and $-i\dot{v} = mv$, so $u(t) = u(0)e^{-imt}$ and $v(t) = v(0)e^{imt}$.

Free field solution of Klein-Gordon: Here $\hbar = 1$. $\varphi(x,t) = Ae^{Et-p\cdot x} = Ae^{\omega_k x^0 - k\cdot x}$ leading to $\varphi(x) = \int \frac{d^3k}{(2\pi)^{3/2}\sqrt{2\omega_k}}(\tilde{\varphi}(k)e^{\omega_k x^0 - k\cdot x} + \tilde{\varphi}(k)^* e^{\omega_k x^0 - k\cdot x})$. Promote $\tilde{\varphi}(k) \to \hat{a}$ and $\tilde{\varphi}(k)^* \to \hat{a}^\dagger$. $\mathcal{L} = \frac{1}{2}\partial_\mu\partial^\mu\varphi - \frac{1}{2}m^2\varphi^2$ and $\pi(x) = \frac{\partial\mathcal{L}}{\partial(\partial_0\varphi)}$. $\hat{\pi}(x) = -i\int \frac{d^3k}{(2\pi)^{3/2}}\sqrt{\frac{\omega_k}{2}}[(\tilde{a}(k)e^{-(\omega_k x^0 - k\cdot x)} - \tilde{a}^\dagger(k)^* e^{\omega_k x^0 - k\cdot x})$. $[x_i, p_j] = i\delta_{ij}$, $[x_i, x_j] = 0$, $[p_i, p_j] = 0$. $|k_1, k_2\rangle = \tilde{a}^\dagger(k_1)\tilde{a}^\dagger(k_2)|00\rangle$. Each $\hat{a}^\dagger(k_i)$ creates a single particle of momentum $\hbar k_i$ and energy $\hbar\omega_k$. $\varphi^+(x) = \int \frac{d^3k}{(2\pi)^{3/2}}\sqrt{\frac{\omega_k}{2}}\hat{a}^\dagger(k)e^{-(\omega_k x^0 - k\cdot x)}$ and positive frequency corresponds to annihilation. $\varphi^-(x) = \int \frac{d^3k}{(2\pi)^{3/2}}\sqrt{\frac{\omega_k}{2}}\hat{a}^\dagger(k)e^{(\omega_k x^0 - k\cdot x)}$ and negative frequency corresponds to creation.

Normalization: $\langle 0|0\rangle = 1$, $\langle k|k'\rangle = \delta(k - k')$ for bosons. $\langle 0|\hat{H}|0\rangle = \langle 0|\int d^3k(N(k) + \frac{1}{2})|0\rangle = \frac{\omega_k}{2}\int d^3k$. *Renormalized:* $\hat{H}_R = \hat{H} - \int d^3k = \int d^3k(\omega_k\hat{a}^\dagger(k)\hat{a}(k)$ and $\langle k|\hat{H}_R|k\rangle = \omega_k$.

Propagators: $\hat{P} = \int d^3k(k[\hat{a}^\dagger(k)\hat{a}(k) + \hat{b}^\dagger(k)\hat{b}(k)])$. $\hat{Q} = \int d^3k[\hat{a}^\dagger(k)\hat{a}(k) + \hat{b}^\dagger(k)\hat{b}(k)]$. $\hat{H} = \int d^3k(\omega_k[\hat{a}^\dagger(k)\hat{a}(k) + \hat{b}^\dagger(k)\hat{b}(k)])$. The number of particles is $\hat{N}_a = \int d^3k[\hat{a}^\dagger(k)\hat{a}(k)]$; the number of anti-particles is $\hat{N}_b = \int d^3k[\hat{b}^\dagger(k)\hat{b}(k)]$. $[\hat{\psi}(x), \hat{\psi}(h)] = i\Delta(x-y)$ is a *propagator*. Feynman propagator is $\Delta_F(x-y) = \langle 0|T\psi(x)\psi(y)|0\rangle = D(x-y), x^0 > y^0$, T is the time ordering operation. Note that an events are *causal* if $[O_1(x), O_2(y)] = 0$ when $(x-y)^2 < 0$.

Momentum space: $\langle x'|\alpha\rangle = \psi_\alpha(x')$, $\langle\beta|\alpha\rangle = \int dx'\langle\beta|x'\rangle\langle x'|\alpha\rangle$. $|\alpha\rangle = \sum_{a'}|a'\rangle\langle a'|\alpha\rangle$, $\langle x'|\alpha\rangle = \sum_{a'}\langle x'|a'\rangle\langle a'|\alpha\rangle$.

$p|\alpha\rangle = \int dx'|x'\rangle(\langle x'|\alpha\rangle - \Delta x' \frac{\partial}{\partial x'}\langle x'|\alpha\rangle$. $p|\alpha\rangle = \int dp|p'\rangle(\langle p'|\alpha\rangle$, $\langle p'|\alpha\rangle = \int dp\langle p|p'\rangle(\langle p'|\alpha\rangle$, $\langle p'|\alpha\rangle = \psi_\alpha(p)$. $p'\langle x'|p\rangle\langle p'|\alpha\rangle$ and thus $p'\langle x'|p\rangle = -i\hbar\frac{\partial}{\partial x'}\langle x'|p'\rangle$ and $\langle x'|p'\rangle = Ne^{i(p'\cdot x')/\hbar}$. $\psi_a(x') = \frac{1}{\sqrt{2\pi\hbar}}\int dp' exp(\frac{i(p'\cdot x')}{\hbar})\phi_a(p')$; $\phi_a(p'))) = \frac{1}{\sqrt{2\pi\hbar}}\int dx' exp(\frac{-i(p'\cdot x')}{\hbar})\psi_a(x')$.

Derivation of Hamiltonian from creation and annihilation operators: $\hat{a}\hat{a}^\dagger = (\frac{m\omega}{2\hbar})[\hat{x}^2 + \frac{\hat{p}^2}{(m\omega)^2} - \frac{i\hat{x}\cdot\hat{p}}{(m\omega)} + \frac{i\hat{x}\cdot\hat{p}}{(m\omega)}] = (\frac{m\omega}{2\hbar})[\hat{x}^2 + \frac{\hat{p}^2}{(m\omega)^2} - \frac{i}{(m\omega)} + \frac{i\hat{x}\cdot\hat{p}}{(m\omega)}] = (\frac{m\omega}{2\hbar})[\hat{x}^2 + \frac{\hat{p}^2}{(m\omega)^2} + \frac{\hbar}{(m\omega)}]$. Similarly, $\hat{a}^\dagger\hat{a} = (\frac{m\omega}{2\hbar})[\hat{x}^2 + \frac{\hat{p}^2}{(m\omega)^2} - \frac{\hbar}{(m\omega)}]$. Combining, $\hat{H} = \frac{1}{2}\hbar\omega[\hat{a}^\dagger\hat{a} + \hat{a}\hat{a}^\dagger] = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2})$. Note, $[\hat{a}, \hat{a}^\dagger] = 1$. Now, put $N = \hat{a}^\dagger\hat{a}$ then $[\hat{a}^\dagger, N] = -\hat{a}^\dagger$ and $[\hat{a}, N] = \hat{a}$. Thus, $N\hat{a} = \hat{a}N - \hat{a} = \hat{a}(N-1)$ and $N\hat{a}\dagger = \hat{a}\dagger(N+1)$. Now, $\langle\psi|N|\psi\rangle \geq 0$ and is 0 iff $\hat{a}|\psi\rangle = 0$. Now suppose λ is an eignevalue of N: $N|\psi\rangle = \lambda|\psi\rangle$. By the above, $N\hat{a}^\dagger|\psi\rangle = \hat{a}^\dagger(\lambda+1)|\psi\rangle$ and $N\hat{a}|\psi\rangle = (\lambda-1)\hat{a}|\psi\rangle$, so $\lambda+1$ and $\lambda-1$ are also an eigenvalues of N corresponding with eigenvectors $\hat{a}\dagger|\psi\rangle$ and $\hat{a}|\psi\rangle$ respectively. Repeated application yields $\hat{a}^n|\psi\rangle$ is an eigenvector of N with eigenvalue $(\lambda-1)\ldots(\lambda-n)$ If $\lambda \notin \mathbb{Z}^+$, $\lambda - n$ is eventually negative and is never 0 but then, $\langle\psi|N|\psi\rangle \leq 0$ eventually which is impossible, so $\lambda \in \mathbb{Z}^+$. Putting $|n\rangle = c_n\hat{a}^\dagger|0\rangle$ with $\langle n|n\rangle = 1$. We get $c_n = \frac{c_{n-1}}{\sqrt{n}}$. $0 = \langle x|\hat{a}|0\rangle = (\frac{(m\omega)}{2\hbar})^{1/2}(\hat{x} + \frac{\hbar}{m\omega}\frac{\partial}{\partial x})\langle x|0\rangle$. $\psi_0(x) = \langle x|0\rangle$ satisfies $(\frac{\partial}{\partial x} + \frac{m\omega}{\hbar})\psi_0(x) = 0$ and $\psi_0(x) = Ne^{\frac{m\omega}{2\hbar}x^2}$ while $\psi_1(x) = \langle x|1\rangle = (\frac{2m\omega}{\hbar})^{1/2}x\psi_0(x)$.

Multiple particles: For a two particle SHO, $H = H_1 + H_2$ with $H_i = \frac{\hat{p}_i^2}{2m} + \frac{1}{2}m\omega^2\hat{x}_i^2$ with $H_i|n\rangle_i = \hbar\omega(n + \frac{1}{2})|n\rangle_i$ and $|n_1, n_2\rangle = |n_1\rangle \otimes |n_2\rangle$ and $H|n_1, n_2\rangle = \hbar\omega(n_1 + n_2 + 1)|n_1, n_2\rangle$.

Identical particles: $Ux_iU^{-1} = x_{\sigma(i)}$, $Up_iU^{-1} = p_{\sigma(i)}$ and $UHU^{-1} = H$ with $H = \sum_i H_i$ and $H_i|\psi_r\rangle = E_r|\psi_r\rangle$. A basis for $\mathcal{H}_1 \otimes \mathcal{H}_2$ is $|\psi_r\rangle_1|\psi_s\rangle_2$; $\frac{1}{\sqrt{2}}(|\psi_r\rangle_1|\psi_s\rangle_2 + |\psi_s\rangle_1|\psi_r\rangle_2), r \neq s$.

Spinless Bosons: For N spinless bosons, $H = \sum_i H_i$. The symmetric basis is $\frac{1}{\sqrt{N!}}\sum_\sigma(|\psi_{\sigma(1)}\rangle_1|\psi_{\sigma(2)}\rangle_2\ldots|\psi_{\sigma(N)}\rangle_N)$. Note that spinless bosons are fully characterized by x, p.

Spin $\frac{1}{2}$ Fermions: State includes spin $|s\rangle$, the full state is $|x\rangle|s\rangle$ with $\psi(x,s) = |x,s\rangle$ and $\psi_s(x) = \langle x,s|\psi\rangle$. The basis for two particles is $\chi_A(s_1,s_2) = \frac{1}{\sqrt{2}}(\chi_{1/2}(s_1)\chi_{-1/2}(s_2) - \chi_{-1/2}(s_1)\chi_{1/2}(s_2))$.

Bell's argument restated: Consider two spin-$\frac{1}{2}$ electrons. $|\uparrow\rangle$ and $|\downarrow\rangle$ are eigenvectors of $S_3 = \frac{1}{2}\hbar\sigma_3$. $\chi_\uparrow = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\chi_\downarrow = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. $\sigma\cdot n = \begin{pmatrix} cos(\theta) & sin(\theta) \\ sin(\theta) & -cos(\theta) \end{pmatrix}$ and $n = (sin(\theta), 0, cos(\theta))$. $\chi_{\uparrow;n} = cos(\frac{\theta}{2})\chi_\uparrow + sin(\frac{\theta}{2})\chi_\downarrow$ and $\chi_{\downarrow;n} = -sin(\frac{\theta}{2})\chi_\uparrow + cos(\frac{\theta}{2})\chi_\downarrow$, set $|\Phi\rangle = \frac{1}{\sqrt{2}}[|\uparrow\rangle_1|\downarrow\rangle_2 + |\downarrow\rangle_1|\uparrow\rangle_2]$. If there are "hidden variables," we'd expect a distribution $0 \leq p(S_z^{(1)}, S_n^{(1)}, S_m^{(1)}, S_z^{(2)}, S_n^{(2)}, S_m^{(2)}) \leq 1$. Define $p_{bc}(b,c) = \sum_a p(a,b,c)$, $p_{ac}(a,c) = \sum_b p(a,b,c)$, $p_{ab}(a,b) = \sum_c p(a,b,c)$. $p_{bc}(1,-1) \leq p_{ab}(1,1) + p_{ac}(-1,-1)$. Applying this to two electrons, $P(S_n^{(1)} = 1, S_m^{(2)} = 1) \leq P(S_z^{(1)} = 1, S_n^{(2)} = -1) + P(S_z^{(1)} = -1, S_m^{(2)} = 1)$. $P(S_n^{(1)} = 1, S_n^{(2)} = -1) = cos^2(\frac{\theta}{2})$ and $P(S_z^{(1)} = 1, S_m^{(2)} = -1) = cos^2(\frac{\phi+\theta}{2})$ which is not generally true.

Definition: The *Compton wavelength* is $\Delta x \geq \frac{\hbar}{mc}$.

Lie Groups: $R(\theta,\hat{z}) = \begin{pmatrix} cos(\theta) & sin(\theta) & 0 \\ -sin(\theta) & cos(\theta) & 0 \\ 0 & 0 & 1 \end{pmatrix}$. $v' = R(\theta,\hat{z})$. $L_z = \frac{1}{i}\frac{\partial R(\theta,\hat{z})}{\partial\theta}_{|\theta=0}$. $R(\theta,\hat{z}) = 1 + \delta\theta L_z$. $SO(3)$ is generated by $\langle L_x, L_y, L_z\rangle$, $R(\theta,\hat{z}) = lim_{N\to\infty}R(\frac{\theta}{N},\hat{z})$. $[L_i, L_j] = i\epsilon_{ijk}L_k$. $J^2|j,m\rangle = j(j+1)|j,m\rangle$, $J_z|j,m\rangle = m|j,m\rangle$. $SU(2)$ acts on spinors. $A = A(\theta,\hat{n}) = exp(i\frac{\theta}{2}\sigma\cdot n) = 1 + i\theta J\cdot n$. $J\cdot n = \frac{1}{i}\frac{\partial A(\theta,\hat{n})}{\partial\theta}_{|\theta=0} =$

$\frac{\sigma}{2}\cdot n$. $\langle \frac{\sigma_x}{2}, \frac{\sigma_y}{2}, \frac{\sigma_z}{2}, \rangle$ is a basis for $SU(2)$.

Representations of symmetry groups: Let G be the symmetry group of a physical system with Hamiltonian H, if $g \in G$ then $[g, H] = 0$ (Note: it is sufficient if this holds on generators.). $\Phi : G \to V_n(F)$ is a representation of the system. Given a Hermitian representation, $\Phi(g)$ of G, $\Phi'(g) = exp(i\Phi(g))$ is a unitary representation. These are called D functions. $\langle j, m'|U(\phi,\theta,\chi)|j,m\rangle = D^{(j)}_{m',m}(\phi,\theta,\chi) = e^{im\phi}d^{(j)}_{m',m}(\theta)e^{-im\chi}$. J^2 acts on a $2j+1$ dimensional Hilbert space. $J_\pm = J_x \pm iJ_y$ and $J_\pm|j,m\rangle = \sqrt{j(j+1)-m(m\pm1)}|j,m\pm1\rangle$. Spin is a representation of $SU(2)$. There is a homomorphism of $SU(2) \to SO(3)$ with kernel $\{\pm1\}$ given by $A(\theta,\hat{n}) \mapsto R(\theta,\hat{n})$ or $\begin{pmatrix} e^{-i\alpha/2} & 0 \\ 0 & e^{i\alpha/2} \end{pmatrix} \mapsto \begin{pmatrix} cos(\alpha) & sin(\alpha) & 0 \\ -sin(\alpha) & cos(\alpha) & 0 \\ 0 & 0 & 1 \end{pmatrix}$. The Klein Gordon equation is invariant under the Lorentz group. The *Poincare group* is the Lorentz group plus translations $T(x) = \Lambda x + a$. $|\Lambda^0_0| \geq 1$.

Subgroup	det	Λ^0_0
$L^\uparrow_+$	1	≥ 1
$L^\downarrow_+$	1	≤ -1
$L^\uparrow_-$	-1	≥ 1
$L^\downarrow_-$	-1	≤ -1

Two fundamental transformations are "rotations" and "boosts"(time change). Rotations, (J_1, J_2, J_3): $\Lambda_R(\theta,\hat{z}) = exp(i\theta)$. Boosts, (K_1, K_2, K_3): $\Lambda_B(\theta,\hat{z}) = exp(\theta)$. $[J^i, J^j] = i\epsilon^{ijk}J^k$, $[J^i, K^j] = i\epsilon^{ijk}K^k$, $[K^i, K^j] = i\epsilon^{ijk}J^k$. $M = exp(\frac{i}{2}\theta\cdot\sigma)exp(\pm\frac{1}{2}\phi\cdot\sigma)$, $\hat{\phi} = \phi\cdot n$, $\hat{\sigma} = \sigma\cdot n$. Type I representation (M): $J = \frac{\sigma}{2}$, $K = -i\frac{\sigma}{2}$. Type II representation $(\overline{M})$: $J = \frac{\sigma}{2}$, $K = -i\frac{\sigma}{2}$. $\begin{pmatrix} \xi \\ \eta \end{pmatrix} \to \begin{pmatrix} M(\Lambda) & 0 \\ 0 & \overline{M}(\Lambda) \end{pmatrix}\begin{pmatrix} \xi \\ \eta \end{pmatrix}$, $\overline{M}(\Lambda) = \epsilon M^*\epsilon^{-1}, \epsilon = i\sigma^2$.

Symmetries and fields: $(t,x) \to (t,-x)$ is the *parity* symmetry. $\phi \to \overline{\phi}^T$ is the *charge conservation* symmetry. Spin 0 scalar fields have Lagrangian $\mathcal{L} = \frac{1}{2}\partial_\mu\phi\partial_\nu\phi - \frac{1}{2}M^2\phi^2$. Spin $\frac{1}{2}$ Dirac fields have Lagrangian $\mathcal{L} = \overline{\phi}(i\partial_\mu\partial_\nu - M)\phi$. Spin 1 vector fields have Lagrangian $\mathcal{L} = -\frac{1}{4}F_{\mu,\nu}F^{\mu,\nu} + \frac{1}{2}m^2V_\mu V^\mu = \frac{\lambda}{2}(\partial_{mu}V^\mu)^2$. The *Poisson Bracket* is $[A,B]_P = \frac{dA}{dq}\frac{dB}{dp} - \frac{dA}{dp}\frac{dB}{dq}$. $\frac{dO}{dt} = [O,H]_P$ and $\frac{dO}{dq} = [O,p]_P$.

Summary:
(1) Spin 0 boson, Klein Gordon equation. $\mathcal{L} = \frac{1}{2}(\dot{\phi}_\alpha\dot{\phi}_\alpha - \mu^2\phi^2)$, $\pi(x) = \frac{\partial\mathcal{L}}{\partial\dot{\phi}}$. $[\phi,\phi^+] = i\hbar c^2\delta(x-x')$. $\phi^+ = \sum_k(\frac{\hbar c^2}{2V\omega_k})^{1/2}a + (k)e^{-ikx/\hbar}$. $H = \sum_k \hbar\omega_k(a^\dagger a(k) + \frac{1}{2})$. $P = \sum_k \hbar k(a^\dagger a(k) + \frac{1}{2})$. Propagator: $[\phi^+,\phi] = i\hbar c\Delta(x-y)$ $\Delta(x) = \frac{ic}{(2\pi)^3}\int d^4k\,\delta(k^2-\mu^2)\epsilon(k)e^{-ikx}$.
(2) Spin 1/2 fermion, Dirac equation. $\mathcal{L} = c\overline{\phi}[c\alpha\cdot(i\hbar\nabla) + \beta mc^2]\phi$, $\pi(x) = \frac{\partial\mathcal{L}}{\partial\dot{\phi}}$. $\{a_r, a_s^\dagger\} = \delta_{rs}$, $\{a_r, a_s\} = 0$. $H = c\int d^3x\overline{\phi}[-i\hbar c\gamma^j\frac{\partial}{\partial x^j} + mc^2]\phi$. $P = -i\hbar\int(\phi^\dagger\nabla\phi(k)$. Propagator: $S_F(x) = \frac{-\hbar}{(2\pi\hbar)^4}\int d^4p\, e^{-ip\cdot x/\hbar}\frac{\gamma^\mu p_\mu + mc}{p^2-m^2c^2+1\epsilon}$.
(3) Spin 1 photon, Maxwell's equation. $\mathcal{L} = -\frac{1}{4}(F_{\mu\nu}F^{\mu\nu} - \frac{1}{c}s_\mu(x)A^\mu(x))$. $[A^\mu(x), A^\mu(x')] = i\hbar x D^{\mu\nu}(x-x')$, $H = \sum_{k,r} d^3x\,\hbar\omega_k\eta_r a_r^\dagger(k)a_r(k)$.

4.8 More on Dirac and QED

The equations: Spin 0 particles are characterized by Klein-Gordon. Spin $\frac{1}{2}$ particles are characterized by Dirac. Spin 1 particles are characterized by Proca.

Dirac: $(i\hbar\gamma^\mu\partial_\mu - mc = 0)$. The time independent solution is $\psi(x) = ae^{-ik\cdot x}u(k)$ for particles and

$\psi(x) = ae^{ik\cdot x}u(k)$ for antiparticles. $uu^\dagger = \frac{2E}{c}$. $N = \sqrt{\frac{E+mc^2}{2}}$. $\gamma^0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\gamma^i = \begin{pmatrix} 0 & \sigma^i \\ -\sigma^i & 0 \end{pmatrix}$. $\psi = \begin{pmatrix} u^{(1)} \\ u^{(2)} \\ v^{(1)} \\ v^{(2)} \end{pmatrix}$. $u^{(1)} = N\begin{pmatrix} 1 \\ 0 \\ \frac{cp_z}{E+mc^2} \\ \frac{c(p_x+ip_y)}{E+mc^2} \end{pmatrix}$. $u^{(2)} = N\begin{pmatrix} 0 \\ 1 \\ \frac{c(p_x+ip_y)}{E+mc^2} \\ \frac{cp_z}{E+mc^2} \end{pmatrix}$. $v^{(1)} = N\begin{pmatrix} \frac{c(p_x-ip_y)}{E+mc^2} \\ \frac{-cp_z}{E+mc^2} \\ 0 \\ 1 \end{pmatrix}$. $v^{(2)} = N\begin{pmatrix} \frac{-cp_z}{E+mc^2} \\ \frac{c(p_x-ip_y)}{E+mc^2} \\ 1 \\ 0 \end{pmatrix}$. For photon, $A_\mu = ae^{ip\cdot x/\hbar}\epsilon^\mu(p)$, ϵ^μ is the polarization vector. $\epsilon^0 = 0$ so $\epsilon \cdot p = 0$, $\epsilon^1 = (1,0,0)$, $\epsilon^2 = (0,1,0)$.

Spinor component	Particle	Spin
$u^{(1)}$	e^-	up
$u^{(2)}$	e^-	down
$v^{(1)}$	e^+	up
$v^{(2)}$	e^+	down

$S = \frac{\hbar}{2}\begin{pmatrix} \sigma & 0 \\ 0 & \sigma \end{pmatrix}$.

The vacuum: The *Casimir effect* is the force between two plates seperated by d due to vacuum fluctuation of the EM field. In QFT, $P = \int \frac{d^3p}{(2\pi)^3} p a_p^\dagger a_p$. We can recover the position operator by $X = \int d^3x (x\phi^\dagger(x)\phi(x)$ giving $X|x\rangle = x|x\rangle$.

Summary:

Characteristic	Electrons	Positrons	Photons
Ket	$ae^{-ip\cdot x/\hbar}u^{(s)}(p)$	$ae^{ip\cdot x/\hbar}v^{(s)}(p)$	$A_\mu = ae^{-i\epsilon\cdot x/\hbar}\epsilon_\mu^{(s)}$
EOS	$(\gamma^\mu p_\mu - mc)u = 0$	$(\gamma^\mu p_\mu + mc)v = 0$	$\Box^2 A^\mu = 0$
Adjoint	$\overline{u}(\gamma^\mu p_\mu - mc) = 0$	$\overline{v}(\gamma^\mu p_\mu + mc) = 0$	-
Constraints	$\overline{u}^{(1)} \cdot u^{(2)} = 0$, $\overline{u}u = 2mc$	$\overline{v}^{(1)} \cdot v^{(2)} = 0$, $\overline{v}v = -2mc$	$p^\mu \epsilon_\mu = 0$
Basis	$\sum_s \overline{u}^{(s)} \cdot u^{(s)} = (\gamma^\mu p_\mu + mc)$	$\sum_s \overline{v}^{(s)} \cdot v^{(s)} = (\gamma^\mu p_\mu - mc)$	$\sum_s \epsilon_i^{(s)}(\epsilon_j^{(s)})^* = \delta_{ij} - \hat{p}_i\hat{p}_j$

Feynman rules for QED: The rules for QED. To calculate $\mathcal{M}$: (1) To eac external line, draw directed segment labeled by momentum,(2) for electron into (out of) vertex use u ($\overline{u}$) switch for positron, (3) use vertex coupling $ig_e\gamma^\mu$, $g_e = e\sqrt{\frac{4\pi}{\hbar c}}$, (4) Use propagators $\frac{i(\gamma^\mu q_\mu + mc)}{q^2 - m^2c^2}$ for e^+, e^- and $\frac{ig_{\mu,\nu}}{q^2}$ for γ, (5) apply δ function $\delta^{(4)}(k_1 + k_2 + k_3)$ (inwards) at each vertex, (6) integrate over internal momentum $\frac{d^4q}{(2\pi)^4}$, (7) cancel the δ's replacing them wiht i, (8) do anti-symmetrization in diagrams interchanging only direction. Example: *electron-electron* scattering $\mathcal{M} = -\frac{g_e^2}{(p_1-p_3)^2}[\overline{u}(3)\gamma^\mu u(1)][\overline{u}(3)\gamma_\mu u(2)] + \frac{g_e^2}{(p_1-p_4)^2}[\overline{u}(4)\gamma^\mu u(1)][\overline{u}(3)\gamma_\mu u(2)]$.

Chapter 5

Quantum Computing

5.1 Basics

$\mathcal{G} = \langle CNOT, X, Y, Z, H, T\rangle$ can be efficiently simulated on a probabalistic computer if there is little entanglement. This is the theorem of *Gottesman-Knill*.

$CNOT : \frac{(|0\rangle+|1\rangle)}{\sqrt{2}}\frac{(|0\rangle-|1\rangle)}{\sqrt{2}} \mapsto \frac{(|0\rangle-|1\rangle)}{\sqrt{2}}\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$. Note that $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$ and $\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$ are eigenvectors of $CNOT$. $CNOT : |b\rangle\frac{(|0\rangle-|1\rangle)}{\sqrt{2}} = (-1)^b|b\rangle\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$ and $CNOT : (\alpha_0|0\rangle + (\alpha_1|1\rangle)\frac{(|0\rangle-|1\rangle)}{\sqrt{2}} = (\alpha_0|)\rangle - \alpha_1|1\rangle)\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$.

Let $U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$. $U_f : |x\rangle\frac{(|0\rangle-|1\rangle)}{\sqrt{2}} = |x\rangle = \frac{(|0\oplus f(x)\rangle-|1\oplus f(x)\rangle)}{\sqrt{2}} = (-1)^{f(x)}|x\rangle\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$ and $U_f : (\alpha_0|0\rangle + (\alpha_1|1\rangle)\frac{(|0\rangle-|1\rangle)}{\sqrt{2}} \mapsto ((-1)^{f(0)}\alpha_0|0\rangle - (-1)^{f(1)}\alpha_1|1\rangle)\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$. H decodes information encoded in the phase.

Proof of no-cloning theorem: Suppose such a unitary transforamtion exists. $U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$ and $U(|\phi\rangle|0\rangle) = |\phi\rangle|\phi\rangle$. On one hand, $U(a|\phi\rangle+b|\psi\rangle) = a|\phi\rangle|\phi\rangle+b|\psi\rangle\psi\rangle)$. On the other hand, $U(a|\phi\rangle+b|\psi\rangle|0\rangle) = (a|\phi\rangle + b|\psi\rangle)(a|\phi\rangle + b|\psi\rangle)$. This is a contradiction. There is no "approximate cloning" either.

Phase Estimation Problem: Given $|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{|y\rangle} e^{2\pi i\omega y}|y\rangle$. ($\omega = \{0,1\}$. $QFT = (|0> + e^{2\pi i 2^{n-1}\omega}|1\rangle)\otimes (|0> + e^{2\pi i 2^{n-2}\omega}|1\rangle)\otimes \ldots A$. $R_n = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^n} \end{pmatrix}$.

Hidden subgroup problem: Let $f : G \to X$, $\exists S < G$ with $f(x) = f(y)$ iff $x + S = y + S$.

Deutsch: $G = \mathbb{Z}_2$, $X = \{0,1\}$. $S = \{0\}$ if f is balenced. $S = \{0,1\}$ if f is constant.

Order Finding: $G = \mathbb{Z}$, $X = H < G$, $r = |a|, a \in H$. $S = r\mathbb{Z}$ so S gets r.

Discrete Log: $G = \mathbb{Z}_r \times \mathbb{Z}_r$, $X = H < G$, $a : a^r = 1$, $b = a^k$, $f(x_1, x_2) = a^{x_1}b^{x_2}$. $f(x_1, x_2) = f(y_1, y_2)$ iff $a^{x_1-y_1}b^{x_2-y_2} = 1$ iff $\langle z_1 - y_1, x_2 - y_2\rangle = (t, -tk), t = 0, 1, \ldots, r-1$. $S = \langle 1, -k\rangle$, $k = log(b)$.

Hidden Linear function: $G = \mathbb{Z} \times \mathbb{Z}$, $g \in S_n$. $h : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_n$ by $h(x, y) = x + ya \pmod n$.

$f = g \circ h$, $G = \mathbb{Z}$, $X = \{0, 1\}$. $S = \langle -a, r \rangle$.

Abelian Stabilizer: G acts on X, $f_x : g \to X$ by $f_x(g) = x^g$. $S = G_x$.

Graph Isomorphism: $G = S_n$ and $\mathcal{G}_n$ is a graph on n vertices. For $\sigma \in G$, $f_{\mathcal{G}}(\sigma(\mathcal{G}))$. The hidden subgroup is the automorphisms of $\mathcal{G}_n$.

$\mathcal{G} = \langle CNOT, X, Y, Z, H, T \rangle$ can be efficiently simulated on a probabalistic computer if there is little entanglement. This is the theorem of *Gottesman-Knill*.

$CNOT : \frac{(|0\rangle+|1\rangle)}{\sqrt{2}} \frac{(|0\rangle-|1\rangle)}{\sqrt{2}} \mapsto \frac{(|0\rangle-|1\rangle)}{\sqrt{2}} \frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$. Note that $\frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$ and $\frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$ are eigenvectors of $CNOT$. $CNOT : |b\rangle \frac{(|0\rangle-|1\rangle)}{\sqrt{2}} = (-1)^b |b\rangle \frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$ and $CNOT : (\alpha_0|0\rangle + (\alpha_1|1\rangle) \frac{(|0\rangle-|1\rangle)}{\sqrt{2}} = (\alpha_0|)\rangle - \alpha_1|1\rangle) \frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$.

Let $U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$. $U_f : |x\rangle \frac{(|0\rangle-|1\rangle)}{\sqrt{2}} = |x\rangle = \frac{(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle)}{\sqrt{2}} = (-1)^{f(x)} |x\rangle \frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$ and $U_f : (\alpha_0|0\rangle + (\alpha_1|1\rangle) \frac{(|0\rangle-|1\rangle)}{\sqrt{2}} \mapsto ((-1)^{f(0)} \alpha_0|0\rangle - (-1)^{f(1)} \alpha_1|1\rangle) \frac{(|0\rangle-|1\rangle)}{\sqrt{2}}$. H decodes information encoded in the phase.