COOPERS THEOREMS

Early in my career I stopped doing mathematical research in the traditional sense and concentrated on developing mathematics curriculum. Being at a brand new university, as Macquarie University was in the 1970's I had enormous freedom to teach what I wanted, especially in the senior years.

As a result I started writing my notes and, in the course of so doing, I developed a certain amount of new material. It could hardly be called 'research' but these are some theorems that may be of interest that you probably won't find anywhere else.

FIRST YEAR LEVEL

THE CUBIC FIT METHOD (Elementary Calculus)

This is an improvement on Simpson's Rule that, provided you know the derivative of the function, gives more accurate results for a similar amount of work. It comes from fitting a cubic to a strip based on the ordinates and derivatives at the endpoints. It doesn't need an even number of strips and consists of the Simpson's Rule formula, plus a 'correction':

$$\int_a^b y\,dx \approx \text{SIMPSON'S ESTIMATE} - \frac{h^2}{12}\,[y']_a^b$$

where h = width of the strips.

For example the percentage errors in the estimates of $\int_1^5 \sqrt{x}\,dx$ with 4 strips are:

Trapezium Rule	0.3%
Simpson's Rule	0.02%
Cubic Fit Method	0.004%

SECOND ORDER EXPANSION (Linear Algebra: Matrices)

This is an improvement on the cofactor method for evaluating determinants. While it involves somewhat less computation its main purpose is to simplify proof of the properties of determinants. If A is a square matrix then $\delta_{ij}^{st}(A)$ is the matrix obtained from A by deleting rows s, t and columns i, j.

$$|A| = \sum_{i<j} (-1)^{1+i+j} \begin{vmatrix} a_{1i} & a_{1j} \\ a_{2i} & a_{2j} \end{vmatrix} .|\delta_{ij}^{12}(A)| .$$

THE GENERALISED TRACE METHOD (Linear Algebra: Matrices)

This computes the coefficients of the characteristic polynomial of a square matrix, without having to evaluate $|\lambda I - A|$, with its error prone calculations, manipulating expressions in λ.

The ***k*-th trace**, $\mathbf{tr}_k\mathbf{(A)}$, is the sum of all the $k \times k$ sub-determinants that can be obtained from A by deleting corresponding rows and columns. So $tr_0(A) = 1$, $tr_1(A)$is the normal trace, and $tr_n(A)$, for an n × n matrix is just |A|. The characteristic polynomial of the $n \times n$ matrix A is:

$$\chi(\lambda) = \lambda^n - tr(A)\lambda^{n-1} + tr_2(A)\lambda^{n-2} + ... + (-1)^{n-k} tr_k(A)\lambda^k + ... + (-1)^n|A|.$$

THE ONE-WAY EUCLIDEAN ALGORITHM (Techniques of Algebra)

The Euclidean Algorithm finds the GCD of two integers, a and b. However if you want to express this in the form ah + bk you have to work backwards through all these calculations. Here is a method whereby enough information is collected along the way to find a suitable h and k once the GCD is obtained.

We perform the calculation in a table with three columns. We begin as follows:

A	**Q**	**B**
a		0
b	q = INT(a,b)	1

Continue as follows:

A	**Q**	**B**
…….	…….	…….
A′	…….	B′
A	q = INT(A′/A)	B
A′ – Aq		B′ – qB

We end as follows:

…….	…….	…….
GCD	q	**k**
0	← STOP	

The first column contains the successive remainders and the last non-zero remainder will be the GCD. In the third column, opposite the GCD will be a suitable value of *k*. Having found *k* the corresponding value of *h* is simply $h = \frac{\text{GCD} - bk}{a}$.

THIRD YEAR LEVEL

THE TOO MANY PRIMES TEST (Galois Theory)

There are many tests for primeness in an integer polynomial – none of them works in the majority of cases. The too many primes test is a useful addition to Eisenstein's method, and all the others.

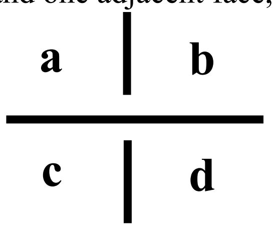
If $f(x) \in \mathbb{Z}[x]$ has degree $n > 5$ and f(m) is prime or ± 1 for at least $n + 3$ integer values of m, the f(x) is prime over $\mathbb{Q}$. For n = 4 or 5 this target is 9. For $n = 2$ or 3, it is $n + 3$. (These targets are best possible.)

COLLINEARITY LEMMA (Geometry)

This is a useful lemma for simplifying certain proofs in Projective Geometry, including Desargue's Theorem and Pappus' Theorem. It is based on the real projective plane being thought of a 1- and 2-dimensional subspaces of R^3 (points and lines respectively). If $P = \langle \mathbf{p} \rangle$, Q, R, S are collinear projective points such that P, Q, R are distinct and $P \neq S$, then for a suitably chosen vector $\mathbf{q}$ and scalar λ we may express the four points as: $P = \langle \mathbf{p} \rangle$, $Q = \langle \mathbf{q} \rangle$, $R = \langle \mathbf{p} + \mathbf{q} \rangle$, $S = \langle \lambda\mathbf{p} + \mathbf{q} \rangle$. Moreover ,if the Euclidean plane is embedded in $\mathbb{R}^3$ and P*, Q*, R* and S* are the corresponding points on the plane, λ is their cross ratio.

ALEXANDER GROUPS (Topology)

Let K be a knot and let M be a map for it. We define an abelian group for the knot in terms of generators and relations as follows. Assign a generator to each face, except for the outside and one adjacent face, which are both assigned 0. At each crossing create a relation as follows:



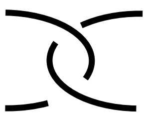
produces the relation **a + b = c + d**. The abelian group with these generators and relations , which I call the Alexander Group, is an invariant of the knot. It can be generalized to links, and for knots it can be generalized to a module over the ring of rational Laurent polynomials in t, by using the relation **t(a + b) + c + d = 0** if the overcrossing is coming from the right. From this it is possible to obtain the Alexander polynomial.

ALEXANDER GROUPS OF CHAINS (Topology)

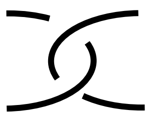
Although this was proved by Simon Byrne, a vacation scholar that I supervised at Macquarie University, I played a small part in it.

A **chain** is a set of two or more non-intersecting closed curves in R^3 where each is linked to the next. (For example, the Olympic logo.)

There are two ways that a pair of adjacent links can occur in a projection of a chain and we'll refer to these as positive and negative connections as follows.



+ve connection



–ve connection

This distinction only occurs at the level of projections because both are equivalent for the chain itself.

Suppose a chain with $n \geq 2$ links has its ends joined. In a projection onto a plane (where the only crossings are those that join each link to its neighbours) let m be the absolute difference between the number of positive and negative connections. The Alexander group of this closed chain is $\mathbb{Z}_2^{\,n-2} \oplus \mathbb{Z}_{2m}$ if $m > 0$ and $\mathbb{Z}_2^{\,n-2} \oplus \mathbb{Z}$ if $m = 0$.
(Here $\mathbb{Z}_2^{\,n-2}$ denotes the direct sum of $n - 2$ copies of $\mathbb{Z}_2$.)

CLASS EQUATIONS

Let t∗n denote n conjugacy classes of size n.

- Let G be a group of order 2N with a conjugacy class of size N. Then N is odd and the class equation for G is $2N = 1 + 2*\left(\frac{N-1}{2}\right) + N$.
- Let G be a group of order 3N with two conjugacy classes of size N. Then $|G'| = N$ and the class equation for G is $3N = 1 + 3t_1 + 3t_2 + \ldots + 3t_k + N + N$ where the class equation for G′ is $N = 1 + t_1*3 + t_2*3 + \ldots + t_k*3$.
- Let G be a group of order pN, where p is prime, with p−1 conjugacy classes of size N. Then G is a Frobenius group with kernel G′ of order N.

POWER AUTOMORPHISMS (Groups)

A power automorphism, θ, of a group is one that fixes every subgroup (i.e. $\theta(x) = x^n$ for all x, but the *n* may vary). Every power automorphism is central (induces the identity automorphism on G/Z(G)).

SYLOW SUBGROUPS OF SYMMETRIC GROUPS (Groups)

Let $G^{(r)}$ denote the wreath product of r copies of G and G^r the direct product of r copies of G. If p is prime and N and $N = a_r a_{r-1} \ldots a_1\, a_0$ in base p notation, the Sylow p-subgroups of S_N are isomorphic to $C_p{}^{(r)a_r} \times C_p{}^{(r-1)a_{r-1}} \times \ldots \times C_p{}^{(2)a_2} \times C_p{}^{a_1}$, where C_p is the cyclic group of order p.

p-ORDER and p-INERTIA (Numbers)

If p is prime and is coprime with m, the **p-order** of m is **u(p, m)**. the smalles positive u such that $p^u \equiv 1 (\mathrm{mod}\ p)$. If p, q are distinct primes the **p-inertia** of q, denoted by **v(p, q)**, is the largest v such that $p^{u(p,q)} \equiv 1 (\mathrm{mod}\ q^v)$.

If $2 < p < q$ are primes then $u(p, q^t) = \begin{cases} u(p, q) \text{ if } 0 < t \le v(p, q) \\ u(p, q)\, q^{t-v(p,q)} \text{ if } t > v(p, q) \end{cases}$.

THE MONOID OF MULTIPLICATIVE FUNCTIONS (Numbers)

A function F(n) on ℕ is multiplicative if F(mn) = F(m)F(n) whenever m, n are coprime. The **Möbius product** F ∗ G of two multiplicative functions F, G is defined by:

$$(F * G)(n) = \sum_{d|n} F(d)G\left(\frac{n}{d}\right) = \sum_{d|n} F\left(\frac{n}{d}\right)G(d) .$$

We can write this symmetrically as $(F * G)(n) = \sum_{cd=n} F(c)G(d)$, and so F ∗ G = G ∗ F for all multiplicative functions.

The set of all multiplicative functions is a commutative monoid under the Möbius product. It has an identity $1:\mathbb{N} \to \mathbb{N}$ defined by $1(n) = \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ otherwise} \end{cases}$.