THE UNIVERSITY OF TORONTO
UNDERGRADUATE MATHEMATICS COMPETITION

March, 2005

Time: $3\frac{1}{2}$ hours

`No aids or calculators permitted.`

It is not necessary to do all the problems. Complete solutions to fewer problems are preferred to partial solutions to many.

1. Show that, if $-\pi/2 < \theta < \pi/2$, then

$$\int_0^\theta \log(1 + \tan\theta \tan x) dx = \theta \log \sec\theta \ .$$

2. Suppose that f is continuously differentiable on $[0,1]$ and that $\int_0^1 f(x)dx = 0$. Prove that

$$2\int_0^1 f(x)^2 dx \le \int_0^1 |f'(x)|dx \cdot \int_0^1 |f(x)|dx \ .$$

3. How many $n \times n$ invertible matrices A are there for which all the entries of both A and A^{-1} are either 0 or 1?

4. Let a be a nonzero real and $\mathbf{u}$ and $\mathbf{v}$ be real 3-vectors. Solve the equation

$$2a\mathbf{x} + (\mathbf{v} \times \mathbf{x}) + \mathbf{u} = \mathbf{O}$$

for the vector $\mathbf{x}$.

5. Let $f(x)$ be a polynomial with real coefficients, evenly many of which are nonzero, which is *palindromic*. This means that the coefficients read the same in either direction, *i.e.* $a_k = a_{n-k}$ if $f(x) = \sum_{k=0}^n a_k x^k$, or, alternatively $f(x) = x^n f(1/x)$, where n is the degree of the polynomial. Prove that $f(x)$ has at least one root of absolute value 1.

6. Let G be a subgroup of index 2 contained in S_n, the group of all permutations of n elements. Prove that $G = A_n$, the alternating group of all even permutations.

7. Let $f(x)$ be a nonconstant polynomial that takes only integer values when x is an integer, and let P be the set of all primes that divide $f(m)$ for at least one integer m. Prove that P is an infinite set.

8. Let $AX = B$ represent a system of m linear equations in n unknowns, where $A = (a_{ij})$ is an $m \times n$ matrix, $X = (x_1, \cdots, x_n)^{\mathbf{t}}$ is an $n \times 1$ vector and $B = (b_1, \cdots, b_m)^{\mathbf{t}}$ is an $m \times 1$ vector. Suppose that there exists at least one solution for $AX = B$. Given $1 \le j \le n$, prove that the value of the jth component is the same for every solution X of $AX = B$ if and only if the rank of A is decreased if the jth column of A is removed.

9. Let S be the set of all real-valued functions that are defined, positive and twice continuously differentiable on a neighbourhood of 0. Suppose that a and b are real parameters with $ab \neq 0$, $b < 0$. Define operators from S to $\mathbf{R}$ as follows:

$$A(f) = f(0) + af'(0) + bf''(0) \ ;$$

$$G(f) = \exp A(\log f) \ .$$

(a) Prove that $A(f) \le G(f)$ for $f \in S$;
(b) Prove that $G(f+g) \le G(f) + G(g)$ for $f, g \in S$;
(c) Suppose that H is the set of functions in S for which $G(f) \le f(0)$. Give examples of nonconstant functions, one in H and one not in H. Prove that, if $\lambda > 0$ and $f, g \in H$, then λf, $f + g$ and fg all belong to H.

10. Let n be a positive integer exceeding 1. Prove that, if a graph with $2n+1$ vertices has at least $3n+1$ edges, then the graph contains a circuit (*i.e.*, a closed non-self-intersecting chain of edges whose terminal point is its initial point) with an even number of edges. Prove that this statement does not hold if the number of edges is only $3n$.

Solutions.

1. Show that, if $-\pi/2 < \theta < \pi/2$, then

$$\int_0^\theta \log(1+\tan\theta\tan x)dx = \theta\log\sec\theta \ .$$

Solution 1. [D. Han]

$$\begin{aligned}\int_0^\theta \log(1+\tan\theta\tan x)dx &= \int_0^\theta \log(1+\tan\theta\tan(\theta-u))du \\ &= \int_0^\theta \log\left[1+\tan\theta\left(\frac{\tan\theta-\tan u}{1+\tan\theta\tan u}\right)\right]du \\ &= \int_0^\theta [\log(1+\tan^2\theta)-\log(1+\tan\theta\tan u)]du \\ &= \theta\log\sec^2\theta - \int_0^\theta \log(1+\tan\theta\tan u)du = 2\theta\log\sec\theta - \int_0^\theta \log(1+\tan\theta\tan x)dx \ .\end{aligned}$$

The desired result follows.

Solution 2.

$$\begin{aligned}\int_0^\theta \log(1+\tan\theta\tan x)dx &= \int_0^\theta [\log(\cos\theta\cos x+\sin\theta\sin x)-\log\cos\theta-\log\cos x]dx \\ &= \int_0^\theta [\log\cos(\theta-x)+\log\sec\theta-\log\cos x]dx \\ &= \int_0^\theta \log\cos(\theta-x)dx+\theta\log\sec\theta-\int_0^\theta \log\cos x dx \\ &= \int_0^\theta \log\cos x dx+\theta\log\sec\theta-\int_0^\theta \log\cos x dx = \theta\log\sec\theta \ .\spadesuit\end{aligned}$$

Solution 3. Let $F(\theta) = \int_0^\theta \log(1+\tan\theta\tan x)dx$. Then, using the substitution $u = \tan x$, we find that

$$\begin{aligned}F'(\theta) &= \log(1+\tan^2\theta)+\int_0^\theta \frac{\sec^2\theta\tan x}{1+\tan\theta\tan x)}dx \\ &= \log\sec^2\theta+\int_0^{\tan\theta}\left[-\frac{\tan\theta}{1+(\tan\theta)u}+\frac{u}{u^2+1}+\frac{\tan\theta}{u^2+1}\right]du \\ &= +2\log\sec\theta+\left[\log(1+(\tan\theta)u+\frac{1}{2}\log(1+u^2)+\tan\theta[\arctan u]\right]_0^{\tan\theta} \\ &= 2\log\sec\theta-\log(1+\tan^2\theta)+\frac{1}{2}\log\sec^2\theta+\theta\tan\theta \\ &= \log\sec\theta+\theta\tan\theta \ .\end{aligned}$$

Also, the derivative of $G(\theta) \equiv \theta\log\sec\theta$ is equal to $\log\sec\theta+\theta\tan\theta$. Since $F'(\theta) = G'(\theta)$ and $F(0) = G(0) = 0$, it follows that $F(\theta) = G(\theta)$ for $-\frac{\pi}{2} < \theta < \frac{\pi}{2}$, as desired.

Comment. It is interesting to observe that

$$\int_0^\theta \log(1+\tan\theta\tan x)dx = \theta\cdot\frac{\log 1+\log\sec^2\theta}{2} \ ,$$

the length of the interval times the average of the integrand values at the endpoint.

2. Suppose that f is continuously differentiable on $[0,1]$ and that $\int_0^1 f(x)dx = 0$. Prove that

$$2\int_0^1 f(x)^2dx \le \int_0^1 |f'(x)|dx\cdot\int_0^1 |f(x)|dx \ .$$

Solution 1.

$$
\begin{aligned}
2\int_0^1 f(x)^2 dx &= \int_0^1 f(x)[2f(x) - f(0) - f(1)]dx \\
&= \int_0^1 f(x)[(f(x) - f(0)) - (f(1) - f(x)]dx \\
&= \int_0^1 f(x)\left[\int_0^x f'(t)dt - \int_x^1 f'(t)dt\right]dx \\
&\le \int_0^1 |f(x)|\left|\int_0^x f'(t)dt - \int_x^1 f'(t)dt\right|dx \\
&\le \int_0^1 |f(x)|\left(\int_0^x |f'(t)|dt + \int_x^1 |f'(t)|dt\right)dx \\
&= \int_0^1 |f(x)|\left(\int_0^1 |f'(t)|dt\right)dx \\
&= \int_0^1 |f'(x)|dx \cdot \int_0^1 |f(x)|dx \ .\spadesuit
\end{aligned}
$$

Solution 2. Let $F(x) = \int_0^x f(t)dt$. Then, integrating by parts, we find that

$$\int_0^1 f^2(x)dx = \Big[f(x)F(x)\Big]_0^1 - \int_0^1 f'(x)F(x)dx = -\int_0^1 f'(x)F(x)dx \ .$$

Hence

$$\int_0^1 f^2(x)dx \le \int_0^1 |f'(x)||F(x)|dx \le \left(\int_0^1 |f'(x)|dx\right) \cdot \sup\{|F(x)| : 0 \le x \le 1\} \ .$$

Now

$$2|F(x)| = |F(x) - F(0)| + |F(1) - F(x)| = |\int_0^1 f(t)dt| + |\int_x^1 f(t)dt| \le \int_0^1 |f(t)|dt \ ,$$

from which the result follows. ♠

3. How many $n \times n$ invertible matrices A are there for which all the entries of both A and A^{-1} are either 0 or 1?

Solution 1. Let $A = (a_{ij})$ and $A^{-1} = (b_{ij})$. Since A and A^{-1} are both invertible, there is at least one 1 in each row and in each column of either of these matrices. Suppose that $1 \le k \le n$. Since $1 = \sum_{j=1}^n a_{kj}b_{jk}$, there is a unique index m for which $a_{km} = b_{mk} = 1$. If $l \ne k$, then $0 = \sum_{j=1}^n a_{lj}b_{jk} = \sum_{j=1}^n a_{kj}b_{jl}$, so that $a_{lm} = b_{ml} = 0$. Thus, the mapping $k \longrightarrow m$ is one-one and each row and each column of each matrix contains exactly one 1. Thus A is a permutation matrix (as is A^{-1}), and there are $n!$ possibilities. ♠

Solution 2. Let $\mathbf{e} = (1, 1, 1, \cdots, 1)^{\mathbf{t}}$. Then each component of $A\mathbf{e}$ is a positive integer. The kth component of $\mathbf{e}$ is the kth component of $A^{-1}(A\mathbf{e})$, namely $\sum_{j=1}^n b_{kj}(A\mathbf{e})j$, where b_{ij} is the (i,j)th component of A^{-1}. Thus

$$1 = \sum_{j=1}^n b_{kj}(A\mathbf{e})j$$

so that there is at most one value of i for which $b_{ki} \ne 0$ and $b_{ki} = (A\mathbf{e})_i = 1$. Since A^{-1} is invertible, there is at least one 1 in each row, so there must be exactly one in each row. Similarly, there is at least one 1 in each column, so that A^{-1} must be a permutation matrix, as must be A. Therefore, there are exactly $n!$ possibilities. ♠

Solution 3. [E. Redelmeier] Let $A = (a_{ij})$ and $A^{-1} = (b_{ij})$. Since $1 = \sum_{j=1}^n a_{ij}b_{ji}$, there is a unique value of j, say $j = \sigma(i)$ for which $a_{ij} = b_{ji} = 1$. Suppose, for $i \ne l$, that $\sigma(i) = \sigma(l)$. Then $0 = \sum_{j=1}^n a_{ij}b_{jl} \ge a_{i\sigma(i)}b_{\sigma(l)l} = 1$, a contradiction. Hence σ is one-one and so a permutation. Suppose, for $k \ne \sigma(i)$, $a_{ik} = a_{i\sigma(i)}$. Then $k = \sigma(l)$, for some index l distinct from i and so $a_{ij}b_{jl} \ge a_{i\sigma(l)}b_{\sigma(l)l} = 1$, a contradiction. Hence each row contains exactly one 1 and, moreover, A is a permutation matrix. So also is A^{-1}. Conversely, each permutation matrix has the desired property, and so the number of matrices is $n!$. ♠

4. Let a be a nonzero real and $\mathbf{u}$ and $\mathbf{v}$ be real 3-vectors. Solve the equation

$$2a\mathbf{x} + (\mathbf{v} \times \mathbf{x}) + \mathbf{u} = \mathbf{O}$$

for the vector $\mathbf{x}$.

Solution 1. Take the dot and cross products by $\mathbf{v}$ to get

$$2a(\mathbf{v}.\mathbf{x}) + \mathbf{v}.\mathbf{u} = 0$$

and

$$2a(\mathbf{v} \times \mathbf{x}) + \mathbf{v} \times (\mathbf{v} \times \mathbf{x}) + \mathbf{v} \times \mathbf{u} = \mathbf{O} \ .$$

The second equation can be manipulated to

$$2a(\mathbf{v} \times \mathbf{x}) + (\mathbf{v}.\mathbf{x})\mathbf{v} - (\mathbf{v}.\mathbf{v})\mathbf{x} + \mathbf{v} \times \mathbf{u} = \mathbf{O}$$

whence

$$\begin{aligned} \mathbf{v} \times \mathbf{x} &= -\frac{1}{2a}[(\mathbf{v}.\mathbf{x})\mathbf{v} - (\mathbf{v}.\mathbf{v})\mathbf{x} + (\mathbf{v} \times \mathbf{u})] \\ &= +\frac{1}{4a^2}(\mathbf{v}.\mathbf{u})\mathbf{v} + \frac{1}{2a}(\mathbf{v}.\mathbf{v})\mathbf{x} - \frac{1}{2a}(\mathbf{v} \times \mathbf{u}) \ . \end{aligned}$$

Therefore

$$2a\mathbf{x} + \mathbf{u} = -\frac{1}{4a^2}(\mathbf{v}.\mathbf{u})\mathbf{v} - \frac{1}{2a}(\mathbf{v}.\mathbf{v})\mathbf{x} + \frac{1}{2a}(\mathbf{v} \times \mathbf{u})$$

which can be rearranged to give

$$[8a^3 + 2a(\mathbf{v}.\mathbf{v})]\mathbf{x} = -(\mathbf{v}.\mathbf{u})\mathbf{v} + 2a(\mathbf{v} \times \mathbf{u}) - 4a^2\mathbf{u} \ .$$

Observe that, since $\mathbf{v} \cdot \mathbf{v} > 0$, the coefficient of $\mathbf{x}$ is nonzero and the same sign as a. ♠

Solution 2. Suppose that $\mathbf{v} = \lambda\mathbf{u}$ for some real λ. Then, since $\mathbf{v} \times \mathbf{x}$ is orthogonal to both $\mathbf{v}$ and $\mathbf{x}$, we must have that $\mathbf{x} = (2a)^{-1}\mathbf{u}$.

Suppose that $\mathbf{v}$ is not a multiple of $\mathbf{u}$. Then we can write $\mathbf{u} = \lambda\mathbf{v} + \mathbf{w}$ where $\mathbf{w} \neq \mathbf{O}$ and $\mathbf{v} \perp \mathbf{w}$. Then $\{\mathbf{v}, \mathbf{w}, \mathbf{v} \times \mathbf{w}\}$ is an orthogonal basis for 3-space. Define the operator

$$T(\mathbf{x}) = 2a\mathbf{x} + (\mathbf{v} \times \mathbf{x}) \ .$$

Then $T(\mathbf{v}) = 2a\mathbf{v}$, $T(\mathbf{w}) = 2a\mathbf{w} + (\mathbf{v} \times \mathbf{w})$, $T(\mathbf{v} \times \mathbf{w}) = 2a(\mathbf{v} \times \mathbf{w}) + \mathbf{v} \times (\mathbf{v} \times \mathbf{w}) = 2a(\mathbf{v} \times \mathbf{w}) - |\mathbf{v}|^2\mathbf{w}$. Then, with respect to this basis, we obtain the equation

$$\begin{pmatrix} 2a & 0 & 0 \\ 0 & 2a & -|\mathbf{v}|^2 \\ 0 & 1 & 2a \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = - \begin{pmatrix} \lambda \\ 1 \\ 0 \end{pmatrix} \ .$$

Hence, the components of $\mathbf{x}$ are given by

$$x = -\frac{\lambda}{2a} \qquad y = \frac{-2a}{4a^2 + |\mathbf{v}|^2} \qquad z = \frac{1}{4a^2 + |\mathbf{v}|^2} \ . ♠$$

Solution 3. Denote the three components of the vectors by subscripts in the usual way. Since $\mathbf{v} \times \mathbf{x} = (v_2x_3 - v_3x_2, v_3x_1 - v_1x_3, v_1x_2 - v_2x_1)$, the given equation is equivalent to the system of scalar equations:

$$2ax_1 - v_3x_2 + v_2x_3 = -u_1$$

$$v_3x_1 + 2ax_2 - v_1x_3 = -u_2$$

$$-v_2x_1 + v_1x_2 + 2ax_3 = -u_3 \ .$$

The determinant D of the coefficients is equal to $2a(4a^2 + |\mathbf{v}|^2)$, and so is nonzero. By Cramer's Rule, we obtain the solution:

$$Dx_1 = -(u_1v_1 + u_2v_2 + u_3v_3)v_1 + 2a(v_2u_3 - v_3u_2) - 4a^2u_1 \ ,$$

$$Dx_2 = -(u_1v_1 + u_2v_2 + u_3v_3)v_2 + 2a(v_3u_1 - v_1u_3) - 4a^2u_2 \ ,$$

$$Dx_3 = -(u_1v_1 + u_2v_2 + u_3v_3)v_3 + 2a(v_1u_2 - v_2u_1) - 4a^2u_3 \ . ♠$$

5. Let $f(x)$ be a polynomial with real coefficients, evenly many of which are nonzero, which is *palendromic*. This means that the coefficients read the same in either direction, *i.e.* $a_k = a_{n-k}$ if $f(x) = \sum_{k=0}^{n} a_kx^k$, or, alternatively

$f(x) = x^n f(1/x)$, where n is the degree of the polynomial. Prove that $f(x)$ has at least one root of absolute value 1.

Solution. If $n = \deg f(x)$ is odd, then k and $n-k$ have opposite parity and

$$f(-1) = \sum \{a_k((-1)^k + (-1)^{n-k}) : 0 \le k < n/2\} = 0 \ .$$

Suppose that $n = 2m$. Then $f(x)$ has $2m+1$ coefficients: m pairs (a_k, a_{n-k}) of equal coefficients $(0 \le k \le m-1)$ and a_m. Since evenly many coefficients are nonzero, we must have that $a_m = 0$. Hence

$$\begin{aligned} f(x) &= \sum_{k=0}^{m-1} a_k(x^k + x^{2m-k}) \\ &= x^m \sum_{k=0}^{m-1} a_k(x^{-(m-k)} + x^{m-k}) \\ &= x^m \sum_{j=1}^{m} a_{m-j}(x^{-j} + x^j) \ . \end{aligned}$$

Then $f(e^{i\theta}) = 2e^{mi\theta}\sum_{j=1}^m a_{m-j}\cos j\theta$. Let $P(\theta) = \sum_{j=1}^m a_{m-j}\cos j\theta$. Then $e^{i\theta}$ is a root of f if and only if $P(\theta) = 0$.

Now $\int_0^{2\pi} P(\theta)d\theta = 0$ and $P(\theta)$ is not constant (otherwise f would be identically 0), so $P(\theta)$ is a continuous real function that assumes both positive and negative values. Hence, by the Intermediate Value Theorem, P must vanish somewhere on the interval $[0, 2\pi]$, and the result follows. ♠

6. Let G be a subgroup of index 2 contained in S_n, the group of all permutations of n elements. Prove that $G = A_n$, the alternating group of all even permutations.

Solution 1. Let $u \in S_n \backslash G$. Since G is of index 2, $uG = Gu$ whence $u^{-1}Gu = G$. Thus, $x^{-1}gx \in G$ for each element g in G. If t is a transposition, than $x^{-1}tx$ runs through all transpositions as x runs through G. Therefore, if G contains a transposition, then G must contain every transposition, and so must be all of S_n, giving a contradiction. Thus, every transposition must belong to uG. Hence, if t_1 and t_2 are two transposition, then $t_1 = g_1u$ and $t_2 = t_2^{-1} = g_2u$ for g_1 and g_2 in G. Hence, $t_1t_2 = (g_1u)(u^{-1}g_2^{-1}) = g_1g_2^{-1} \in G$. Thus, G contains every even permutation, and so contains A_n. The result follows.

Solution 2. As in Solution 1, we see that G must be normal, and so must be the kernel of a homomorphism ϕ from S_n into the multiplicative group $\{1, -1\}$. Suppose that $x \in S_n$ and x has order m, then $1 = \phi(x^m) = (\phi(x))^m$, whence m is even or $x \in G$. It follows that every element of odd order must belong to G, and so in particular, G must contain all $3-$cycles. Since $(a, b)(a, c) = (a, b, c)$ and $(a, b)(c, d) = (a, b, c)(a, d, c)$ (multiplying from the left), every product of a pair of transpositions and hence every even permutation is a product of $3-$cycles. Hence G contains all even permutations and so must coincide with A_n.

7. Let $f(x)$ be a nonconstant polynomial that takes only integer values when x is an integer, and let P be the set of all primes that divide $f(m)$ for at least one integer m. Prove that P is an infinite set.

Solution 1. Suppose that $p_k(x)$ is a polynomial of degree k assuming integer values at $x = n, n+1. \cdots, n+k$. Then, there are integers c_i for which

$$p_k(x) = c_{k,0}\binom{x}{k} + c_{k,1}\binom{x}{k-1} + \cdots + c_{k,k}\binom{x}{0} \ .$$

To see this, first observe that $\binom{x}{k}$, $\binom{x}{k-1}$, $\cdots$, $\binom{x}{0}$ constitute a basis for the vector space of polynomials of degree not exceeding k. So there exist *real* $c_{k,i}$ as specified. We prove by induction on k that the $c_{k,i}$ must in fact be integers. The result is trivial when $k = 0$. Assume its truth for $k \ge 0$. Suppose that

$$p_{k+1}(x) = c_{k+1,0}\binom{x}{k+1} + \cdots + c_{k+1,k+1}$$

takes integer values at $x = n, n+1, \cdots, n+k+1$. Then

$$p_{k+1}(x+1) - p_{k+1}(x) = c_{k+1,0}\binom{x}{k} + \cdots + c_{k+1,k}$$

is a polynomial of degree k which taken integer values at $n, n+1, \cdots, n+k$, and so $c_{k+1,0}, \cdots, c_{k+1,k}$ are all integers. Hence,

$$c_{k+1,k+1} = p_{k+1}(n) - c_{k+1,0}\binom{n}{k+1} - \cdots c_{k+1,k}\binom{n}{1}$$

is also an integer. ♣ (This is more than we need; we just need to know that the coefficients of $f(x)$ are all rational.)

Let $f(x)$ be multiplied by a suitable factorial to obtain a polynomial $g(x)$ with integer coefficients. The set of primes dividing values of $g(m)$ at integers m is the union of the set of primes for f and a finite set, so it is enough to obtain the result for g. Note that g assumes the values 0 and 1 only finitely often. Suppose that $g(a) = b \neq 0$ and let $P = \{p_1, p_2, \cdots, p_r\}$ be a finite set of primes. Define

$$h(x) = \frac{g(a + bp_1p_2 \cdots p_r x)}{b} \ .$$

Then $h(x)$ has integer coefficients and $h(x) \equiv 1 \pmod{p_1p_2 \cdots p_r}$. There exists an integer u for which $h(u)$ is divisible by a prime p, and this prime must be distinct from $p_1, p_2, \cdots, p_r$. The result follows. ♠

Solution 2. Let $f(x) = \sum_k^n a_k x_n$. The number $a_0 = f(0)$ is rational. Indeed, each of the numbers $f(0)$, $f(1)$, $\cdots$, $f(n)$ is an integer; writing these conditions out yields a system of $n+1$ linear equations with integer coefficients for the coefficients a_0, a_1, $\cdots$, a_n whose determinant is nonzero. The solution of this equation consists of rational values. Hence all the coefficients of $f(x)$ are rational. Multiply $f(x)$ by the least common multiple of its denominators to get a polynomial $g(x)$ which takes integer values whenever x is an integer. Suppose, if possible, that values of $f(x)$ for integral x are divisible only by primes p from a finite set Q. Then the same is true of $g(x)$ for primes from a finite set P consisting of the primes in Q along with the prime divisors of the least common multiple. For each prime $p \in P$, select a positive integer a_p such that p^{a_p} does not divide $g(0)$. Let $N = \prod\{p^{a_p} : p \in P\}$. Then, for each integer u, $g(Nu) \not\equiv 0 \pmod{N}$. However, for all u, $g(Nu) = \prod p^{b_p}$, where $0 \leq b_p \leq a_p$. Since there are only finitely many numbers of this type, some number must be assumed by g infinitely often, yielding a contradiction. (Alternatively: one could deduce that $g(Nu) \leq N$ for all u and get a contradition of the fact that $|g(Nu)|$ tends to infinity with u.) ♠

Solution 3. [R. Barrington Leigh] Let n be the degree of f. `Lemma.` Let p be a prime and k a positive integer. Then $f(x) \equiv f(x + p^{nk}) \pmod{p^k}$. `Proof by induction on the degree.` The result holds for $n = 0$. Assume that it holds for $n = m - 1$ and $f(x)$ have degree m. Let $g(x) = f(x) - f(x-1)$, so that the degree of $g(x)$ is $m - 1$. Then

$$\begin{aligned} f(x + p^{nk}) - f(x) &= \sum_{i=1}^{p^{nk}} g(x+i) \\ &= \sum_{i=1}^{p^{(n-1)k}} (g(x+i) + g(x+i+p^{(n-1)k}) + \ldots + g(x+i+(p^k-1)p^{(n-1)k}) \\ &\equiv \sum_{i=1}^{p^{(n-1)k}} p^k g(x+i) \equiv 0 \ , \end{aligned}$$

$\pmod{p^k}$. [Note that this does not require the coefficients to be integers.] ♣

Suppose, if possible, that the set P of primes p that divide at least one value of $f(x)$ for integer x is finite, and that, for each $p \in P$, the positive integer a is chosen so that p^a does not divide $f(0)$. Let $q = \prod\{p^a : p \in P\}$. Then p^a does not divide $f(0)$, nor any of the values $f(q^n)$ for positive integer n, as these are all congruent modulo p^a. Since any prime divisor of $f(q^n)$ belongs to P, it must be that $f(q^n)$ is a divisor of q. But this contradicts the fact that $|f(q^n)|$ becomes arbitrarily large with n. ♠

8. Let $AX = B$ represent a system of m linear equations in n unknowns, where $A = (a_{ij})$ is an $m \times n$ matrix, $X = (x_1, \cdots, x_n)^{\mathbf{t}}$ is an $n \times 1$ vector and $B = (b_1, \cdots, b_m)^{\mathbf{t}}$ is an $m \times 1$ vector. Suppose that there exists at least one solution for $AX = B$. Given $1 \leq j \leq n$, prove that the value of the jth component is the same for every solution X of $AX = B$ if and only if the rank of A is decreased if the jth column of A is removed.

Solution 1. Let $C_1, C_2, \cdots, C_n$ be the n columns of A. Suppose that the dimension of the span of these columns is reduced when C_j is removed. Then C_j is not a linear combination of the other C_i. Thus, if $AX = AY = B$ and $Z = X - Y$, then $AZ = O$. This means that $z_1C_1 + z_2C_2 + \cdots + z_jC_j + \cdots + z_nC_n = 0$. Because C_j is not a linear combination of the other C_i, we must have that $z_j = 0$, *i.e.* that $x_j = y_j$.

On the other hand, if the dimension of the span is the same whether or not C_j is present, then C_j must be a linear combination of the remaining C_i. In this case, there is a vector Z with a nonzero value of z_j for which $AZ = z_1C_1 + \cdots + z_jC_j + \cdots + z_nC_n = O$. Thus if X is a solution of $AX = B$, then $X + Z$ is a second solution with a different value of the jth component. ♠

Solution 2. As in the first solution, we observe that every solution of $AX = B$ has the same jth entry if and only if every solution of $AX = O$ has zero in the jth position.

Suppose that every solution of $AX = O$ has 0 in the jth position. Let A_j the the matrix A with the jth column removed and X_j be the vector X with the jth entry removed. Then there is a linear isomorphism between the solutions of $AX = 0$ and $A_jX_j = 0$, where $X \to X_j$ is defined by suppressing the jth entry. Since the target space of A_j has dimension $n - 1$. we find that

$$n - \text{rank } A = \text{nullity } A = \text{nullity } A_j = (n-1) - \text{rank } A_j \ ,$$

whence rank $A_j =$ rank $A - 1$.

On the other hand, suppose that there are solutions of $AX = O$ for which the jth component fails to vanish. Each solution of $A_j Y = 0$ lifts to a solution of $AX = 0$ by inserting the entry 0 after the $(j-1)$th position of Y. However, this lifting does not get all the solutions, so that

$$n - \text{rank } A = \text{nullity } A > \text{nullity } A_j = (n-1) - \text{rank } A_j$$

whence rank $A_j >$ rank $A - 1$. Since, always, the rank of A_j does not exceed that of A, we must have that the ranks of A_j and A are equal. The desired result follows. ♠

9. Let S be the set of all real-valued functions that are defined, positive and twice continuously differentiable on a neighbourhood of 0. Suppose that a and b are real parameters with $ab \neq 0$, $b \leq 0$. Define operators from S to $\mathbf{R}$ as follows:

$$A(f) = f(0) + af'(0) + bf''(0) \ ;$$
$$G(f) = \exp A(\log f) \ .$$

(a) Prove that $A(f) \leq G(f)$ for $f \in S$;
(b) Prove that $G(f + g) \leq G(f) + G(g)$ for $f, g \in S$;
(c) Suppose that H is the set of functions in S for which $G(f) \leq f(0)$. Give examples of nonconstant functions, one in H and one not in H. Prove that, if $\lambda > 0$ and $f, g \in H$, then λf, $f + g$ and fg all belong to H.

Solution. (a) The result if clear if $A(f) \leq 0$. Suppose that $A(f) > 0$. We have that $(\log f)' = f'/f$ and $(\log f)'' = (f''/f) - (f'/f)^2$, so that

$$A(\log f) = \log f(0) + \frac{af'(0)}{f(0)} + \frac{bf''(0)}{f(0)} - b\left(\frac{f'(0)}{f(0)}\right)^2 .$$

We have that

$$\begin{aligned}
\log A(f) &= \log f(0) + \log\left(1 + \frac{af'(0)}{f(0)} + \frac{bf''(0)}{f(0)}\right) \\
&\leq \log f(0) + \frac{af'(0)}{f(0)} + \frac{bf''(0)}{f(0)} \\
&= A(\log f) + b\left(\frac{f'(0)}{f(0)}\right)^2 \leq A(\log f) \ .
\end{aligned}$$

(b) Note that, for any functions $u, v \in S$,

$$G(uv) = \exp A(\log u + \log v) = \exp[A(\log u) + A(\log v)] = \exp A(\log u) \cdot \exp A(\log v) = G(u)G(v) \ .$$

Similarly $G(u/v) = G(u)/G(v)$. From (a), we have the inequalities

$$A\left(\frac{f}{f+g}\right) \leq G\left(\frac{f}{f+g}\right) \qquad \text{and} \qquad A\left(\frac{g}{f+g}\right) \leq G\left(\frac{g}{f+g}\right) .$$

Adding these two inequalities yields

$$1 \leq \frac{G(f) + G(g)}{G(f+g)}$$

from which the desired result follows.

(c) Suppose that $\lambda > 0$ and $f, g \in H$. Then

$$G(\lambda f) = G(\lambda)G(f) = \lambda G(f) \leq \lambda f(0) \ ;$$

$$G(fg) = G(f)G(g) \leq f(0)g(0) = (fg)(0) \ ;$$
$$G(f+g) \leq G(f) + G(g) \leq f(0) + g(0) = (f+g)(0) \ .$$

Suppose that $a \neq 0$, and let $f(x) = e^{kx}$. Then $G(f) = e^{ka}$. If $ka > 0$, then $f \notin H$; if $ka < 0$, then $f \in H$. Suppose that $a = 0$, and let $f(x) = e^{kx^2}$. Then $G(f) = e^{2kb}$. If $k < 0$, then $f \notin H$; if $k > 0$, then $f \in H$. ♠

10. Let n be a positive integer exceeding 1. Prove that, if a graph with $2n+1$ vertices has at least $3n+1$ edges, then the graph contains a circuit (*i.e.*, a closed non-self-intersecting chain of edges whose terminal point is its initial point) with an even number of edges. Prove that this statement does not hold if the number of edges is only $3n$.

Solution 1. If there are two vertices joined by two separate edges, then the two edges together constitute a chain with two edges. If there are two vertices joined by three distinct chains of edges, then the number of edges in two of the chains have the same parity, and these two chains together constitute a circuit with evenly many edges. We establish the general result by induction.

The result can be checked for $n = 2$. Suppose that it holds for $2 \leq n \leq m-1$. We may assume that we have a graph G that contains no instances where two separate edges join the same pair of vertices and no two vertices are connected by more than two chains. Since $3n + 1 > 2n$, the graph is not a tree, and therefore must contain at least one circuit. Consider one of these circuits, L. If it has evenly many edges, the result holds. Suppose that it has oddly many edges, say $2k + 1$ with $k \geq 1$. Since any two vertices in the circuit are joined by at most two chains (the two chains that make up the circuit), there are exactly $2k + 1$ edges joining pairs of vertices in the circuit. Apart from the circuit, there are $(2m + 1) - (2k + 1) = 2(m - k)$ vertices and $(3m + 1) - (2k + 1) = 3(m - k) + k \geq 3(m - k) + 1$ edges.

We now create a new graph G', by coalescing all the vertices and edges of L into a single vertex v and retaining all the other edges and vertices of G. This graph G' contains $2(m - k) + 1$ vertices and at least $3(m - k) + 1$ edges, and so by the induction hypothesis, it contains a circuit M with an even number of edges. If this circuit does not contain v, then it is a circuit in the original graph G, which thus has a circuit with evenly many edges. If the circuit does contain v, it can be lifted to a chain in G joining two vertices of L by a chain of edges in G'. But these two vertices of L must coincide, for otherwise there would be three chains joining these vertices. Hence we get a circuit, *all* of whose edges lie in G'; this circuit has evenly many edges. The result now follows by induction.

Here is a counterexample with $3n$ edges. Consider $2n + 1$ vertices partitioned into a singleton and n pairs. Join each pair with an edge and join the singleton to each of the other vertices with a single edge to obtain a graph with $2n + 1$ vertices, $3n$ edges whose only circuits are triangles. ♠

Solution 2. [J. Tsimerman] For any graph H, let $k(H)$ be the number of circuits minus the number of components (two vertices being in the same component if and only if they are connected by a chain of edges). Let G_0 be the graph with $2n + 1$ vertices and no edges. Then $k(G_0) = -(2n + 1)$. Suppose that edges are added one at a time to obtain a succession G_i of graphs culminating in the graph $G = G_{3n+1}$ with $2n + 1$ vertices and $3n + 1$ edges. Since adding an edge either reduces the number of components (when it connects two vertices of separate components) or increases the number of circuits (when it connects two vertices in the same component), $k(G_{i+1}) \geq k(G_i) + 1$. Hence $k(G) \geq -(2n + 1) + (3n + 1) = n$. Thus, the number of circuits in G is at least equal to the number of components in G plus n, which is at least $n + 1$. Thus, G has at least $n + 1$ circuits.

Since $3(n + 1) > 3n + 1$, there must be two circuits that share an edge.

A counterexample can be obtained by taking a graph with vertices $A_1, \cdots, A_n, B_0, B_1, \cdots, B_n$, with edges joining the vertex pairs (A_i, B_{i-1}), (A_i, B_i) and (B_{i-1}, B_i) for $1 \leq i \leq n$. ♠