Solutions

1 Extra questions to think about:

1. Can we obtain a similar expression when $\mathcal{D}$ is even?
2. Is $\mathcal{F}(n, \mathcal{D})$ always even?

Given a sequence A, let $\overline{A}$ denote the subset of sequences for which the distance, d, between A and the sequences satisfies $0 \leq d \leq \frac{\mathcal{D}-1}{2}$. (For example, if $n = 7, \mathcal{D} = 3$, then for a sequence A say 0000000, $\overline{A} = 0000000, 0000001, 0000010, ..., 1000000$.) Clearly,

$$|\overline{A}| = \sum_{i=0}^{\frac{\mathcal{D}-1}{2}} \binom{n}{i}.$$

Suppose $T_{\mathcal{D}}$ has m elements, $A_1, A_2, ..., A_m$, and consider their associated subsets $\overline{A}_1, \overline{A}_2, ..., \overline{A}_m$.

We shall now prove that no two of these subsets overlap, for if a sequence B were to belong to both $\overline{A}_i$ and $\overline{A}_j$, changing not more than $\frac{\mathcal{D}-1}{2}$ places in A_i would give B and changing not more than $\frac{\mathcal{D}-1}{2}$ places in B gives A_j, and hence the distance between A_i and A_j would not exceed $\mathcal{D} - 1$, a contradiction since A_i and A_j belong to $T_{\mathcal{D}}$.

Hence we have

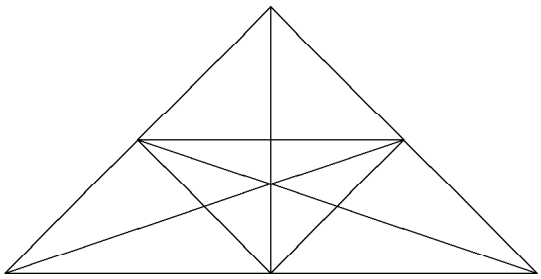
$$m \sum_{i=0}^{\frac{\mathcal{D}-1}{2}} \binom{n}{i} \leq 2^n$$

or

$$\mathcal{F}(n, \mathcal{D}) = m \leq \left\lfloor \frac{2^n}{\sum_{i=0}^{\frac{\mathcal{D}-1}{2}} \binom{n}{i}} \right\rfloor.$$

(i) $\mathcal{F}(5, 3) \leq 5$. We will prove that $\mathcal{F}(5, 3) = 4$. Indeed, we may assume without loss of generality that 00000 is in the desired subset, for if it is not, we can then select an arbitrary sequence, say 10100 from the subset and interchange the 1's to 0's, and suitably interchanging the corresponding respective positions of the other sequences in the subset. So say 00000 is in the desired subset. Let us consider the sequences that are of at least distance 3 from it. They are namely {11100, 11010, 11001, 10110, 10101, 10011, 01110, 01101, 01011, 00111}, {11110, 11101, 11011, 10111, 01111}, {11111}. Notice that if 11111 is also in the subset, we cannot accommodate any other sequences. Also, since the distance between any two elements in the second subset is 2, we can at most accommodate one such sequence in our subset. Similarly, the distance between any two elements in the first subset is either 2 or 4. A direct check reveals we can at most accommodate two such sequences in our desired subset, and hence $\mathcal{F}(5, 3) \leq 4$. But $\{00000, 01011, 11100, 10111\}$ is such a 4 element subset and hence $\mathcal{F}(5, 3) = 4$.

(ii) $\mathcal{F}(7, 3) \leq 16$. This is a bit easier with the aid of the Fano Plane. The following illustration isn't entirely accurate, and more accurate representations can be found on the Internet. Here is the weblink:
http://mathworld.wolfram.com/FanoPlane.html
Just try to understand what they are saying, and you can probably also work out why such a configuration works for the $(7, 3)$ case.



If we assign a value 1, 2, ..., 7 to each of the 7 vertices (the 3 vertices of the triangles, the midpoints of the 3 sides and the centroid) of the 7_3 configuration, say counter-clockwise from the top vertex, with the centroid assigned 7, then we can obtain the incidence matrix from 0000000. Each line contains three of the numbers 1, 2, ..., 7, and all we need to do is to put 1's in these places and 0's everywhere else (consider 2, 4, 6 to be a straight line):

$$\begin{bmatrix} 0000000 \\ 1110000 \\ 0011100 \\ 1000110 \\ 1001001 \\ 0010011 \\ 0100101 \\ 0101010 \end{bmatrix}$$

This set contributes 8 sequences to our desired subset, and for the remaining 8 members, we can use the complements of these, that is the sequences obtained by interchanging the 0's and 1's.

$$\begin{bmatrix} 1111111 \\ 0001111 \\ 1100011 \\ 0111001 \\ 0110110 \\ 1101100 \\ 1011010 \\ 1010101 \end{bmatrix}$$

Denote the first set by X and the second set by Y. The distance between 2 members of Y is hence automatically 3 or 4, as the distance between their antecedents is 3 or 4; the only question is whether some member of X is closer than 3 to some member of Y. One can either go about verifying these 16 elements satisfies our condition by checking each member of X with each member of Y and be done with it, or make the following observation.

The complementary pair $P = 0000000$ and $P' = 1111111$ are best considered separately. Since each member of Y has at least 4 1's, the distance from P to a member of Y is at least 4; similarly P' is at least a distance 4 from any member of X. Also, the distance between any sequence and its complement is 7, and so it remains only to check the distance between a member A of $\{X - P\}$ and a sequence B' from $\{Y - P'\}$ which is not the complement of A.

A direct check reveals that the distance between A and any other member of its own section $\{X - P\}$ is always exactly 4. Similarly, for any two members of $\{Y - P'\}$. Now consider the complement A' of A. A' belongs to Y, and we have just noted

that B' agrees with A' in exactly 3 places u, v, w. Since all the places in A' need reversing to give A, then A must differ from B' in exactly these three places u, v, w and the solution is complete.

2 For $n \geq 2$, let $h(x) = x^{n-1} + ... + x + 1$ and let

$$f(x) = a_{2n-1}x^{2n-1} + ... + a_1 x + a_0$$

be a degree $(2n-1)$ polynomial. First we claim that $f(x)$ is divisible by $h(x)$ if and only if

$$a_{2n-1} + a_{n-1} = a_{2n-2} + a_{n-2} = ... = a_n + a_0.$$

For $1 \leq i \leq n-1$, let w_i be the distinct nth roots of unity other than 1. Since $h(x)(x-1) = x^n - 1$, the w_i are the roots to $h(x)$. So $h(x)|f(x)$ if and only if $f(w_i) = 0$ for all w_i. Let

$$g(x) = (a_{2n-1} + a_{n-1})x^{n-1} + (a_{2n-2} + a_{n-2})x^{n-2} + ... + (a_n + a_0).$$

Since $w_i^n = 1$, we have $w_i^{2n-1} = w_i^{n-1}$, $w_i^{2n-2} = w_i^{n-2}$, ..., and $w_i^n = w_i^0$. Then $g(w_i) = f(w_i)$ for all i, so $h(x)$ divides $f(x)$ if and only if it divides $g(x)$. But this occurs if and only if

$$a_{2n-1} + a_{n-1} = a_{2n-2} + a_{n-2} = ... = a_n + a_0.$$

as claimed.
Suppose that there are N sets of n pairs of distinct integers from $1, 2, ..., 2m$ such that the n pairs have the same sum. In any set, the pairs are disjoint since the numbers in each pair have the same sum. Then there are N sets to choose from and $n!$ ways to choose which pairs from the set correspond to which pairs (a_i, a_{i-n}). Also for each of the n pairs, there are 2 ways to assign the values. Therefore, there are a total of $2^n n!N$ such polynomials. Now it suffices to show that

$$N = 4\binom{m+1}{n+1} - 3\binom{m}{n}.$$

Let $S = \{1, 2, ..., 2m\}$. For a positive integer $k \leq 2m$, there are $\lfloor (k-1)/2 \rfloor$ pairs of distinct integers from S that add up to k; the $k-1$ pairs $(1, k-1), (2, k-2), ..., (k-1, k)$ count each pair twice as well as a possible $(k/2, k/2)$ pair. If $4m > k > 2m$, then there are $\lfloor (4m-k+1)/2 \rfloor$ pairs of distinct integers that add up to k by a similar argument. As k ranges from $3 = 1 + 2$ to $4m - 1 = (2m-1) + 2m$, the number of pairs of distinct integers that add up to k are

$$1, 1, 2, 2, ..., m-1, m-1, m, m-1, m-1, ..., 2, 2, 1, 1.$$

Now a set of n pairs of distinct integers from $1, 2, ..., 2m$ that share the same sum is simply a set of n pairs of the $\lfloor (k-1)/2 \rfloor$ or $\lfloor (4m-k+1)/2 \rfloor$ pairs above. So the number of such sets is equal to

$$\begin{aligned} & 2\binom{1}{n} + 2\binom{2}{n} + ... + \binom{m}{n} + ... + 2\binom{2}{n} + 2\binom{2}{1} \\ = \; & 4\left(\binom{1}{n} + 2\binom{2}{n} + ... + \binom{m-1}{n} + \binom{m}{n}\right) - 3\binom{m}{n} \\ = \; & 4\binom{m+1}{n+1} - 3\binom{m}{n}. \end{aligned}$$

and this completes our proof.

3 Extra questions:

1. Show that for $n \geq 3$, the maximum possible number of MPs who are satisfied with their salaries M satisfies the following inequality: $M \leq \lfloor \frac{2n^2+2n-2}{3} \rfloor$
2. Can we exhibit such a seating? I think we have to consider modulo 4.

We shall show that at most 72 MP's are content with their salaries. Let us represent the members of parliament with a square grid of 10x10 points, and label each point with the salary of the corresponding MP. Let us draw arrows between neighbouring points such that the arrow is directed from the smaller to the larger number.

Then let a be the number of satisfied MP's sitting in the corners, b the number of those sitting at the sides of the square, and c the number of those sitting inside.

The number of arrows is 180. There is at most one arrow originating at any satisfied MP, and there will be at least one point where no arrow originates, the MP with the largest salary (obviously satisfied). Hence the number of arrows originating at satisfied MP's is at most $a + b + c - 1$.

There are at most $(4 - a)2$ arrows from the $4 - a$ dissatisfied MP's in the corners, at most $(32 - b)3$ from the $32 - b$ dissatisfied MP's along the sides, and at most $(64 - c)4$ from those $(64 - c)$ sitting inside. The total number of arrows is thus

$$180 \leq (a + b + c - 1) + (4 - a)2 + (32 - b)3 + (64 - c)4$$

that is, $a + 2b + 3c \leq 179$ The one with the lowest salary out of the 36 MP's around the circumference is necessarily dissatisfied, thus $a + b \leq 35$. It is also obvious that $a \leq 4$. By adding the inequalities, we have

$$3(a + b + c) = (a + 2b + 3c) + (a + b) + a \leq 179 + 35 + 4 = 218.$$

That is, $a+b+c \leq 72$. Hence, the number of satisfied MP's cannot be greater than 72.

The diagram shows the case when there are exactly 72 MP's who are content with their salaries. Sorry guys, I can't draw a really nice one so I just represent it by the following arrays of numbers, with 1 being the one with the smallest salary. Those that are dissatisfied are from 1 - 28.

$$\begin{bmatrix} (91)(92)(93)(94)(95)(96)(97)(98)(99)(100) \\ (90)(01)(29)(02)(30)(03)(31)(04)(32)(05) \\ (89)(33)(06)(34)(07)(35)(08)(36)(09)(37) \\ (88)(10)(38)(40)(41)(43)(44)(46)(47)(48) \\ (87)(49)(11)(39)(12)(42)(13)(45)(14)(50) \\ (86)(15)(51)(16)(52)(17)(53)(18)(54)(55) \\ (85)(65)(64)(62)(61)(59)(58)(56)(19)(71) \\ (84)(20)(63)(21)(60)(22)(57)(23)(70)(72) \\ (24)(66)(25)(67)(26)(68)(27)(69)(28)(73) \\ (83)(82)(81)(80)(79)(78)(77)(76)(75)(74) \end{bmatrix}$$

4 Extra question:

1. Can we do use the same argument for other inequalities involving these symmetric polynomials? Essentially this method provides us with an alternative transformation of variables.

Consider the polynomial

$$f(x) = (x - a_1)(x - a_2)..(x - a_n)$$

Then $f(x)$ has n positive real (not necessarily distinct) roots. Therefore $f'(x)$ has $(n-1)$ positive real (not necessarily distinct) roots. Denote them by $b_1, b_2, ..., b_{n-1}$. Now

$$f(x) = x^n - (\sum a_i)x^{n-1} + (\sum a_i a_j)x^{n-2} + ... + (-1)^{n-1}(\sum_{i=1}^{n} \prod_{j \neq i} a_j n)x + (-1)^n \prod a_i.$$

Hence

$$f'(x) = nx^{n-1} - (n-1)(\sum a_i)x^{n-2} + (n-2)(\sum a_i a_j)x^{n-3} + ... + (-1)^{n-1}(\sum_{i=1}^{n} \prod_{j \neq i} a_j n).$$

Now comparing the coefficients (by Vieta's Theorem) we have

$$b_1 b_2 ... b_{n-1} = \frac{\sum_{i=1}^{n} \prod_{j \neq i} a_j}{n}$$

and

$$\sum b_i b_j = \frac{n-2}{n} \sum a_i a_j$$

Then by the $AM \geq GM$ inequality we have

$$\frac{\sum b_i b_j}{\binom{n-1}{2}} \geq \sqrt[\binom{n-1}{2}]{(b_1 b_2 ... b_{n-1})^{n-2}} = (b_1 b_2 ... b_{n-1})^{\frac{2}{n-1}}$$

Substituting back for the a_i'sand rearranging we obtain

$$\sqrt[n-1]{\frac{\sum_{i=1}^{n} \prod_{j \neq i} a_j}{n}} \leq \sqrt{\frac{2 \sum_{1 \leq i < j \leq n} a_i a_j}{n(n-1)}}.$$

When $n = 2$, we get the reverse of the $AM \leq GM$ inequality, hence $n = 2$ does not work. (as differentiating a polynomial of degree 2 with leave us with a linear factor from which our argument does not include.) Equality holds for all $n \geq 3$, with equality for all a_i when $n = 3$ and when $a_1 = a_2 = ... = a_n \forall n \geq 4$.

5 (a) Observe that

$$\begin{aligned} f(x) &\equiv (x^2 + x)^{2^n} + 1 \\ &\equiv x^{2^{n+1}} + x^{2^n} + 1 \equiv (x^2 + x + 1)^{2^n} (\text{mod} 2); \end{aligned}$$

Since $x^2 + x + 1$ is ireeducible in $Z_2[x]$, if $f(x)$ does factor into two nonconstant factors p and q, then we may assume without loss of generality that

$$p(x) \equiv (x^2 + x + 1)^{2^{n-1}+z} \equiv x^{2^n+2z} + x^{2^{n-1}+z} + 1 (\text{mod} 2),$$

$$q(x) \equiv (x^2 + x + 1)^{2^{n-1}-z} \equiv x^{2^n-2z} + x^{2^{n-1}-z} + 1 (\text{mod} 2).$$

Thus, if we write

$$p(x) = a_{2^n+2z} x^{2^n+2z} + ... + a_0, q(x) = b_{2^n-2z} x^{2^n-2z} + ... + b_0,$$

then $a_{2^n+2z}, a_{2^{n-1}+z}, a_0, b_{2^n-2z}, b_{2^{n-1}-z}, b_0$ are odd and all the other coefficients are even. Since f is monic, we may assume without loss of generality that

$a_{2^n+2z} = b_{2^n+2z} = 1$; also $a_0 b_0 = f(0) = 1$, but f as no real roots (since $f > 0$ for all $n > 1$), hence $a_0 > 0, b_0 > 0$ and $a_0 = b_0 = 1$. Now expanding pq and taking (mod 2), we have

$$a_{2^n+2z} \equiv a_{2^n+2^{n-1}+z} \equiv a_{2^{n-1}+z} \equiv b_{2^n-2z} \equiv b_{2^n+2^{n-1}-z} \equiv b_{2^{n-1}-z} \equiv 0(\text{mod}2).$$

Since each of the terms are odd, such a relation can only hold when 2 of the terms are equivalent. Now suppose $z > 0$. Let us consider the term a_{2^n+2z}.

Clearly,

$$2^n + 2z > 2^{n-1} + z, 2^n + 2z > 2^n - 2z, 2^n + 2z > 2^{n-1} - z,$$

and if $2^n + 2z = 2^n + 2^{n-1} - z$, then we have $2^{n-1} = 3z$, which is impossible. So we must have $2^n + 2z = 2^n + 2^{n-1} + z$, or equivalently, $z = 2^{n-1}$. But if $z = 2^{n-1}$, then we obtain the trivial factorization of f, which is not what we desire. Hence $q = 0$ and f must factor into two polynomials of degree 2^n each.

Alternatively, note that $f(x) = g(h(x))$, where $h(x) = x^2 + x$ and $g(y) = y^{2^n} + 1$. Since

$$g(y+1) = (y+1)^{2^n} + 1 = y^{2^n} + \left(\sum_{k=1}^{2^n-1} \binom{2^n}{k} y^k \right) + 2,$$

and $\binom{2^n}{k}$ is even for $1 \leq k \leq 2^n - 1$, g is irreducible by Eisenstein's criterion. Now let p be a nonconstant factor of f, and let r be a root of p. Then $g(h(r)) = f(r) = 0$. Hence $s = h(r)$ is a root of g. Since $s = r^2 + r \in Q(r)$, we have $Q(s) \subset Q(r)$, so

$$\text{deg}p \geq [Q(r) : Q] \geq [Q(s) : Q] = \text{deg}g = 2^n.$$

Thus every factor of f has degree at least 2^n. Therefore if f is reducible, we can write $f(x) = p(x)q(x)$ where p and q have degree 2^n.

As above,

$$\begin{aligned} f(x) &\equiv (x^2 + x)^{2^n} + 1 \\ &\equiv x^{2^{n+1}} + x^{2^n} + 1 \equiv (x^2 + x + 1)^{2^n} (\text{mod}2); \end{aligned}$$

since $x^2 + x + 1$ is irreducible in $Z_2[x]$, by unique factorization we must have

$$p(x) \equiv q(x) \equiv (x^2 + x + 1)^{2^{n-1}} \equiv x^{2^n} + x^{2^{n-1}} + 1(\text{mod}2).$$

Thus, if we write

$$p(x) = a_{2^n} x^{2^n} + ... + a_0, q(x) = b_{2^n} x^{2^n} + ... + b_0,$$

then $a_{2^n}, a_{2^{n-1}}, a_0, b_{2^n}, b_{2^{n-1}}, b_0$ are odd and all the other coefficients are even. Since f is monic, we may assume without loss of generality that $a_{2^n} = b_{2^n} = 1$; also $a_0 b_0 = f(0) = 1$, but f as no real roots (since f ¿ 0 for all n ¿ 1), hence $a_0 > 0, b_0 > 0$ and $a_0 = b_0 = 1$. Therefore,

$$\begin{aligned} &(\{x^{2^n+2^{n-1}}\} + \{x^{2^{n-1}}\})(g(x)h(x)) \\ &\qquad \equiv \left(\sum_{i=2^{n-1}}^{2^n} a_i b_{2^n+2^{n-1}-i} \right) + \left(\sum_{i=0}^{2^{n-1}} a_i b_{2^{n-1}-i} \right) \\ &\qquad \equiv a_{2^n} b_{2^{n-1}} + a_{2^{n-1}} b_{2^n} + a_0 b_{2^{n-1}} + a_{2^{n-1}} b_0 \\ &\qquad \equiv 2(a_{2^{n-1}} + b_{2^{n-1}}) \\ &\qquad \equiv 0(\text{mod}4) \end{aligned}$$

as $a_{2^{n-1}} + b_{2^{n-1}}$ is even. But

$$(\{x^{2^n+2^{n-1}}\} + \{x^{2^{n-1}}\})(f(x)) = \binom{2^n}{2^{n-1}} = 2\binom{2^n-1}{2^{n-1}-1},$$

and $\binom{2^n-1}{2^{n-1}-1}$ is odd by Lucas's Theorem, so

$$(\{x^{2^n+2^{n-1}}\} + \{x^{2^{n-1}}\})(f(x)) \equiv 2(\mathrm{mod}4)$$

a contradiction. Hence f is irreducible.

(b) A polynomial $f(x) \in \mathbf{Z}[x]$ factors into a product of two polynomials of lower degrees in $\mathbf{Q}[x]$ if and only if it has such a factorization with polynomials of the same degrees in $\mathbf{Z}[x]$.
Proof: Consider $f(x) \in \mathbf{Q}[x]$, let

$$\begin{aligned} f(x) &= \frac{a_0}{b_0} + \frac{a_1}{b_1}x + ... + \frac{a_n}{b_n}x^n, a_i, b_i \in \mathbf{Z}, b_i \neq 0 \\ &= \frac{1}{b_1 b_2 ... b_n}\sum_{i=0}^{n} a_i \prod_{k\neq i} b_k x^i \\ &= \frac{r}{s}(c_0 + c_1 x + ...c_n x^n), r, s, c_i \in \mathbf{Z} \end{aligned}$$

where $r = \gcd(a_i \prod_{k\neq i})$, $s = b_0 b_1 ... b_n$, and $\gcd(c_0, c_1, ..., c_n) = 1$.
Hence $f(x) = cf^*(x)$, where $c \in \mathbf{Q}$ and $f^*(x) \in \mathbf{Z}[x]$. Let us call $f^*(x)$ a primitive polynomial.
Lemma:
The product of two primitive polynomials is again a primitive polynomial.
Proof:
Let $g(x), h(x) \in \mathbf{Z}[x]$ be primitive polynomials. Let

$$\begin{aligned} g(x) &= a_0 + a_1 x + ...a_n x^n \\ h(x) &= b_0 + b_1 x + ...b_m x^m \\ g(x)h(x) &= c_0 + c_1 x + ... + c_{m+n} x^{m+n} \end{aligned}$$

Since $g(x)$ and $h(x)$ are primitive polynomials, there exists a prime p such that p does not divide all the coefficients of $g(x)$ and $h(x)$. Let a_i and b_j be the first coefficients of $g(x)$ and $h(x)$ not divisible by p. Then

$$a_j b_j = c_{i+j} - (a_0 b_{i+j} + ... + a_{i-1} b_{j+1} + a_{i+1} b_{j-1} + ... + a_{i+j} b_0).$$

Since $p|(a_0 b_{i+j} + ... + a_{i-1} b_{j+1})$, $p|(a_{i+1} b_{j-1} + ... + a_{i+j} b_0)$, we have

$$p|(a_0 b_{i+j} + ... + a_{i-1} b_{j+1} + a_{i+1} b_{j-1} + ... + a_{i+j} b_0).$$

Suppose $p|c_{i+j}$, then we must have $p|a_j b_j$, which is a contradiction. Hence p does not divide $a_j b_j$ and we are done.

Now write $f(x) = cf^*(x)$, and suppose that $f(x) = g(x)h(x)$, with $g(x), h(x) \in \mathbf{Q}[x]$. Also, we can write $g(x) = ag^*(x), h(x) = bh^*(x)$, where $a, b \in \mathbf{Q}$ and $g^*(x), h^*(x)$ are primitive. Then we have

$$f(x) = cf^*(x) = abg^*(x)h^*(x)$$

Let $ab = \frac{u}{v}$, with $\gcd(u,v) = 1$, $u, v \in \mathbf{Z}, v > 0$. Then $vcf^*(x) = ug^*(x)h^*(x)$, and since the product of two primitive polynomials is also primitive, $g^*(x)h^*(x)$ is primitive. It follows that $v|u$, but since $\gcd(u,v) = 1$, $v > 0$ that we must have $v = 1$. Then $f(x) = cf^*(x) = [ug^*(x)]\,[h^*(x)]$, and this completes the proof.

Theorems

1. **Eisenstein's Criterion**:
Let $p \in Z$ be a prime. Suppose that $f(x) = a_n x^n + ... + a_0$ is in $Z\,[x]$, and $a_n \neq 0 \pmod p$, but $a_i = 0 \pmod p$ for all $i < n$, with $a_0 \neq 0 \pmod p$. Then $f(x)$ is irreducible over Q.

2. **Lucas's Theorem**:
Let p be a prime. Let a and b be two positive integers such that

$$a = a_k p^k + a_{k-1} p^{k-1} + ... + a_1 p + a_0,$$

$$b = b_k p^k + b_{k-1} p^{k-1} + ... + b_1 p + b_0,$$

where $0 \leq a_i, b_i < p$ are integers, then

$$\binom{a}{b} \equiv \binom{a_k}{b_k}\binom{a_{k-1}}{b_{k-1}}...\binom{a_1}{b_1}\binom{a_0}{b_0} \pmod p.$$

Ok, as a bonus question... haha this one is evil...

For a natural number k, let $p(k)$ denote the smallest prime number which does not divide k. If $p(k) > 2$, define $q(k)$ to be the product of all primes less than $p(k)$, otherwise let $q(k) = 1$. Consider the sequence

$$x_0 = 1; x_{n+1} = \frac{x_n p(x_n)}{q(x_n)}, n = 0, 1, 2, ...$$

Determine all integers n such that $x_n = 2003$.
I have mentioned to a couple of you about this... , those who know what is the idea behind this sequence, establish the claim that I told you.

Here's another of my original creations, and it illustrates this fact: That a polynomial which can be factorised modulo p for all primes p need not be factorisable over the rationals. However, the converse is true, that if a polynomial is reducible over the rationals, then it must be reducible modulo p.

Given any integer $m > 2$, with $m \equiv 2 \pmod 4$, can the polynomial

$$f(x) = x^4 - mx^2 + 1$$

be expressed as a product of two nonconstant polynomials with

(i) rational coefficients?
(ii) coefficients from $\{0, 1, ..., p-1\}$, and where addition and multiplication are carried out modulo p, for every prime p?

Enjoy!