Sydney University Mathematical Society
Problems Competition 2003

Solutions.

1. Notice that $2^2 = 4$, $12^2 = 144$, $38^2 = 1444$ and $2538^2 = 6441444$.

(i) Show that there is no integer x such that $x^2 = \ldots 4444$ in its decimal representation.

(ii) Find a number n such that the last four digits of n^2 are 4144.

(iii) Show that for each $k \geq 1$ there is a number x such that the last k digits of x^2 consist of 1's and 4's only.

(iv) What can one say if 1 and 4 are replaced by other pairs of digits?

Solution. A quick solution to (i) and (ii) is as follows: (i) If $x^2 = \ldots 4444$, then $x^2 \equiv 4444 \pmod{10000}$, and so $x^2 \equiv 12 \pmod{16}$. But the squares mod 16 are just 0, 1, 4 and 9. (ii) The smallest number n with this property is $n = 1012$.

But for the more difficult parts (iii) and (iv) of the question, SUMS cannot improve on the following solution, due to Stewart Wilcox (Sydney University):

Let $D = \{0, 1, \ldots, 9\}$, $O = \{1, 3, 5, 7, 9\}$, $E = \{2, 4, 6, 8\}$ and $S = \{0, 1, 4, 5, 6, 9\}$. Pick any integer x and let y be the last digit of x^2, so $y \in D$ and $x^2 \equiv y \pmod{10}$. Then there exists $z \in D$ with $x \equiv z \pmod{10}$. In fact we can choose $z \leq 5$ by replacing x with $-x$ if necessary, as we will still have $y \equiv x^2 \pmod{10}$. But then $y \equiv z^2 \pmod{10}$, so squaring $0, 1, \ldots, 5$ we see that $y \in S$. Hence the last digit of any square must be in S. Note that each element of S is achievable as the last digit of a square, as

$$\begin{aligned} 0^2 &\equiv 0 \pmod{10}, \\ 1^2 &\equiv 1 \pmod{10}, \\ 2^2 &\equiv 4 \pmod{10}, \\ 5^2 &\equiv 5 \pmod{10}, \\ 4^2 &\equiv 6 \pmod{10}, \\ 3^2 &\equiv 9 \pmod{10}. \end{aligned}$$

Let X be the set of subsets $A \subseteq D$ such that for any positive integer k there exists a perfect square with the last k digits belonging to A. That is, $A \in X$ if and only if for any $k > 0$ there exist integers x, y with $x^2 \equiv y \pmod{10^k}$ and $y \in \sum_{i=0}^{k-1} 10^i A$. We will show that $A \in X$ if and only if either $0 \in A$ or A satisfies the following conditions:

$$\begin{aligned} A \cap S &\neq \emptyset \quad \text{and} \\ A \cap E &\neq \emptyset \quad \text{and} \\ |A| &\geq 2 \quad \text{and} \\ A &\not\subseteq \{2, 6, 8\} \quad \text{and} \\ A &\not\subseteq \{3, 5, 7, 8\}. \end{aligned}$$

First assume $A \in X$. If $0 \in A$ we are done, so assume otherwise. Setting $k = 1$, there exists $x \in \mathbb{Z}$ and $a \in A$ with $x^2 \equiv a \pmod{10}$. Thus $a \in S$, so $A \cap S \neq \emptyset$. Now setting $k = 2$, we have $x^2 \equiv 10a + b \pmod{100}$ for some $x \in \mathbb{Z}$ and $a, b \in A$. If $b \in E$ then $A \cap E \neq \emptyset$ as required. Otherwise $b \notin E$, so $b \in O$ as $b \neq 0$. Again $b \in S$, so $b \in O \cap S = \{1, 5, 9\}$. In particular $b \equiv 1 \pmod{4}$, so $x^2 \equiv 10a + b \equiv 2a + 1 \pmod{4}$. Squaring $0, 1, 2$ shows that any square must be $\equiv 0$ or $1 \pmod{4}$, so a is even. Since

$a \in A$ we have $a \neq 0$, so $a \in E$. Hence in either case $A \cap E \neq \emptyset$ as required. Next we show that $A \not\subseteq \{2, 6, 8\}$. Assume otherwise. Then setting $k = 2$, for some $x \in \mathbb{Z}$ we have $x^2 \equiv 10a + b \pmod{100}$ with $a, b \in A$. But then $b \in S$ and $b \in A \subseteq \{2, 6, 8\}$, so $b = 6$. Also $a \in A \subseteq \{2, 6, 8\}$ so a is even, giving $x^2 \equiv 10a + b \equiv 6 \equiv 2 \pmod{4}$, contradiction. Assume $|A| \leq 1$. Since $A \cap S \neq \emptyset$ we can pick $a \in A \cap S$, giving $A = \{a\}$. Also $A \cap E \neq \emptyset$ so $a \in E \cap S = \{4, 6\}$. If $a = 6$ then $A \subseteq \{2, 6, 8\}$, contradiction. Thus $a = 4$, so setting $k = 4$ we can pick $x \in \mathbb{Z}$ with $x^2 \equiv 4444 \pmod{10^4}$. Clearly x is even so let $x = 2y$, giving $y^2 \equiv 1111 \pmod{2500}$. In particular $y^2 \equiv 1111 \equiv 3 \pmod{4}$, contradiction. Note that we have shown $A = \{4\}$ fails at $k = 4$, a fact which will be used later. Hence $|A| \geq 2$ as required. Finally assume $A \subseteq \{3, 5, 7, 8\}$. Setting $k = 2$ we have $x^2 \equiv 10a + b \pmod{100}$ for some $x \in \mathbb{Z}$ and $a, b \in A$. Thus $b \in S \cap A \subseteq \{5\}$, so $b = 5$. Since x^2 is then odd, we must have $x^2 \equiv 1 \pmod{4}$. Thus $10a \equiv x^2 - 5 \equiv 0 \pmod{4}$, so a is even. But $a \in A \subseteq \{3, 5, 7, 8\}$, giving $a = 8$. Hence $x^2 \equiv 85 \equiv 0 \pmod{5}$, so $x = 5y$ for some $y \in \mathbb{Z}$. Thus $85 \equiv x^2 \equiv 0 \pmod{25}$, contradiction, so the 5 conditions are satisfied as required.

Conversely, assume first that $0 \in A$. Then for any $k > 0$, setting $x = 10^k$ and $y = 0$ we have $x^2 \equiv y \pmod{10^k}$ and $y \in \sum_{i=0}^{k-1} 10^i A$, as required. Now assume $0 \notin A$ but that A satisfies the above 5 conditions. We will first consider the special case $A \cap S = \{5\}$, so $A \subseteq \{2, 3, 5, 7, 8\}$. But $A \not\subseteq \{3, 5, 7, 8\}$, so $2 \in A$. We will inductively construct $x_k \in \mathbb{Z}$ with $x_k \equiv 15 \pmod{25}$ and

$$x_k^2 \equiv 225 + \sum_{i=3}^{k-1} 5 \times 10^i \pmod{5^{k+1}}$$

for all $k \geq 3$. When $k = 3$ let $x_3 = 515$, so $x_3^2 = 225 + 265000$ and $5^4 | 265000$ as required. Now assume x_k has been constructed for some $k \geq 3$, and let

$$225 + \sum_{i=3}^{k-1} 5 \times 10^i - x_k^2 = 5^{k+1} l$$

where $l \in \mathbb{Z}$. Let $x_{k+1} = x_k + 10^k + 5^k l$. We have

$$2x_k \equiv 30 \equiv 5 \pmod{25}$$

Multiplying by $10^k + 5^k l$, which is divisible by 5^k, this gives

$$2x_k(10^k + 5^k l) \equiv 5 \times 10^k + 5^{k+1} l = 225 + \sum_{i=3}^{k} 5 \times 10^i - x_k^2 \pmod{5^{k+2}}$$

Also since $k \geq 3$ we have $2k \geq k + 3 > k + 2$, so $5^{k+2} | 5^{2k}$. Hence $(10^k + 5^k l)^2 \equiv 0 \pmod{5^{k+2}}$, giving

$$x_{k+1}^2 = x_k^2 + 2x_k(10^k + 5^k l) + (10^k + 5^k l)^2 \equiv 225 + \sum_{i=3}^{k} 5 \times 10^i \pmod{5^{k+2}}$$

as required. Also $25 | 5^k | (10^k + 5^k l)$ since $k \geq 3$, so we still have $x_{k+1} \equiv 15 \pmod{25}$. Hence x_k has been constructed inductively. Next we construct $y_k \in \mathbb{Z}$ inductively with

$$y_k^2 \equiv 225 + \sum_{i=3}^{k-1} 5 \times 10^i \pmod{2^k}$$

for all $k \geq 3$. When $k = 3$ let $y_3 = 1$, giving $y_3^2 = 1 \equiv 225 \pmod 8$. Now assume y_k has been constructed for some $k \geq 3$. Then

$$225 + \sum_{i=3}^{k} 5 \times 10^i - y_k^2 \equiv 5 \times 10^k \equiv 0 \pmod{2^k}$$

Let $225 + \sum_{i=3}^{k} 5 \times 10^i - y_k^2 = 2^k l$, and $y_{k+1} = y_k + 2^{k-1} l$. Since $k \geq 3$, we have $2(k-1) \geq k+1$. Hence $(2^{k-1} l)^2 \equiv 0 \pmod{2^{k+1}}$, so

$$y_{k+1}^2 = y_k^2 + 2^k l + (2^{k-1} l)^2 \equiv 225 + \sum_{i=3}^{k} 5 \times 10^i \pmod{2^{k+1}}$$

as required. By the Chinese Remainder Theorem, since 5^k and 2^k are coprime, we can now find $z_k \in \mathbb{Z}$ with $z_k \equiv x_k \pmod{5^k}$ and $z_k \equiv y_k \pmod{2^k}$. Then

$$z_k^2 \equiv x_k^2 \equiv 225 + \sum_{i=3}^{k-1} 5 \times 10^i \pmod{5^k}$$
$$z_k^2 \equiv y_k^2 \equiv 225 + \sum_{i=3}^{k-1} 5 \times 10^i \pmod{2^k}$$

Again using that 2^k and 5^k are coprime, and since $10^k = 2^k \times 5^k$, this gives

$$z_k^2 \equiv 225 + \sum_{i=3}^{k-1} 5 \times 10^i \pmod{10^k}$$

for $k \geq 3$. Clearly the $k = 3$ case implies the $k = 1, 2$ cases, so $A \in X$. Now assume $A \cap S \neq \{5\}$. We will inductively construct a sequence $a_i \in A$ such that $a_0 \in S \setminus \{5\}$ and for all $k \geq 1$,

$$\text{There exists } x \in \mathbb{Z} \quad \text{with } x^2 \equiv \sum_{i=0}^{k-1} a_i 10^i \pmod{2^k} \tag{1}$$

First assume $A \cap O \neq \emptyset$. We also have $A \cap E \neq \emptyset$, so there exist $b, c \in A$ with b odd and c even. Since $A \cap S \neq \emptyset$ or $\{5\}$, there exists $a_0 \in A \cap S$ with $a_0 \neq 5$. But because $a_0 \in S$ there exists $x \in \mathbb{Z}$ with $x^2 \equiv a_0 \pmod{10}$. Thus $x^2 \equiv a_0 \pmod 2$, and the statement is true for $k = 1$. Assume we have constructed $a_0, \ldots, a_{k-1}$ for some $k \geq 1$ with

$$x^2 \equiv \sum_{i=0}^{k-1} a_i 10^i \pmod{2^k}$$

for some $x \in \mathbb{Z}$. Then $x^2 - \sum_{i=0}^{k-1} a_i 10^i \equiv 0$ or $2^k \pmod{2^{k+1}}$. In the former case let $a_k = c$. Then

$$x^2 \equiv \sum_{i=0}^{k-1} a_i 10^i \equiv \sum_{i=0}^{k-1} a_i 10^i + a_k 10^k \equiv \sum_{i=0}^{k} a_i 10^i \pmod{2^{k+1}}$$

since $2^{k+1} | a_k 2^k | a_k 10^k$. In the latter case let $a_k = b$, so $a_k 10^k \equiv 2^k \pmod{2^{k+1}}$. Then

$$x^2 \equiv \sum_{i=0}^{k-1} a_i 10^i + 2^k \equiv \sum_{i=0}^{k-1} a_i 10^i + a_k 10^k \equiv \sum_{i=0}^{k} a_i 10^i \pmod{2^{k+1}}$$

As required. Hence we have constructed a_i inductively. Now assume $A \cap O = \emptyset$. Since $0 \notin A$ this gives $A \subseteq E$. But $A \not\subseteq \{2, 6, 8\}$, so $4 \in A$. Also $|A| \geq 2$, so there exists $b \in A$ with $b \neq 4$. Then $b \in \{2, 6, 8\}$. Assume $b \in \{2, 6\}$, so $b \equiv 2 \pmod 4$. We will construct a sequence a_i satisfying the stronger condition

$$\text{There exists } x \in \mathbb{Z} \quad \text{with } x^2 \equiv \sum_{i=0}^{k-1} a_i 10^i \pmod{2^{k+1}}$$

Clearly this will imply (1). When $k = 1$ we can take $a_0 = 4 \in A \cap S$ and $x = 2$, giving $2^2 = 4 \equiv 4 \pmod 4$ as required. Assume such $a_0, \ldots, a_{k-1}$ have been constructed for some $k \geq 1$. Then

$$x^2 - \sum_{i=0}^{k-1} a_i 10^i \equiv 0 \quad \text{or } 2^{k+1} \pmod{2^{k+2}}$$

In the former case set $a_k = 4 \in A$, so $2^{k+2} | a_k 10^k$. Then

$$x^2 \equiv \sum_{i=0}^{k-1} a_i 10^i \equiv \sum_{i=0}^{k-1} a_i 10^i + a_k 10^k = \sum_{i=0}^{k} a_i 10^i \pmod{2^{k+2}}$$

In the latter case set $a_k = b$, so $a_k \equiv 2 \pmod 4$ gives $a_k 10^k \equiv 2^{k+1} \pmod{2^{k+2}}$. Then

$$x^2 \equiv \sum_{i=0}^{k-1} a_i 10^i + 2^{k+1} \equiv \sum_{i=0}^{k-1} a_i 10^i + a_k 10^k = \sum_{i=0}^{k} a_i 10^i \pmod{2^{k+2}}$$

As required. Finally assume $b = 8$. In this case we will construct a_i so that

$$\text{There exists } x \in \mathbb{Z} \quad \text{with } x^2 \equiv \sum_{i=0}^{k-1} a_i 10^i \pmod{2^{k+2}}$$

Again this will imply (1). As before we can set $a_0 = 4$ and $x = 2$ for the $k = 1$ case. Assume such $a_0, \ldots, a_{k-1}$ have been constructed for some $k \geq 1$. Then

$$x^2 - \sum_{i=0}^{k-1} a_i 10^i \equiv 0 \quad \text{or } 2^{k+2} \pmod{2^{k+3}}$$

In the former case set $a_k = 8 \in A$, so $2^{k+3} | a_k 10^k$. Then

$$x^2 \equiv \sum_{i=0}^{k-1} a_i 10^i \equiv \sum_{i=0}^{k-1} a_i 10^i + a_k 10^k = \sum_{i=0}^{k} a_i 10^i \pmod{2^{k+3}}$$

In the latter case set $a_k = 4 \in A$, so $a_k \equiv 4 \pmod 8$ gives $a_k 10^k \equiv 2^{k+2} \pmod{2^{k+3}}$. Then

$$x^2 \equiv \sum_{i=0}^{k-1} a_i 10^i + 2^{k+2} \equiv \sum_{i=0}^{k-1} a_i 10^i + a_k 10^k = \sum_{i=0}^{k} a_i 10^i \pmod{2^{k+3}}$$

As required. Thus in each case we have inductively constructed a sequence satisfying $5 \neq a_0 \in S$ and (1) for each k. Next we show by induction on k that for all $k \geq 1$ there exists $x \in \mathbb{Z}$ with

$$x^2 \equiv \sum_{i=0}^{k-1} a_i 10^i \pmod{5^k}$$

Since $a_0 \in S$, there exists $x \in \mathbb{Z}$ with $x^2 \equiv a_0 \pmod{10}$. Thus $x^2 \equiv a_0 \pmod{5}$, giving the $k = 1$ case. Assume the statement is true for some $k \geq 1$, and pick such x. Then

$$\sum_{i=0}^{k} a_i 10^i - x^2 \equiv a_k 10^k \equiv 0 \pmod{5^k}$$

Let $\sum_{i=0}^{k} a_i 10^i - x^2 = 5^k l$ where $l \in \mathbb{Z}$. Since $a_0 \in D$ and $a_0 \neq 0, 5$, we have $5 \nmid a_0$. Thus

$$x^2 \equiv \sum_{i=0}^{k-1} a_i 10^i \equiv a_0 \not\equiv 0 \pmod{5}$$

So $5 \nmid x$. Since 5 is prime there exists $m \in \mathbb{Z}$ with $xm \equiv 1 \pmod{5}$. Let $y = x + 3lm5^k$. Since $k \geq 1$ we have $2k \geq k + 1$, so $(3lm5^k)^2 \equiv 0 \pmod{5^{k+1}}$. Also $6lmx \equiv l \pmod{5}$ so multiplying by 5^k gives

$$y^2 = x^2 + 2 \times x \times 3lm5^k + (3lm5^k)^2 \equiv x^2 + 5^k l = \sum_{i=0}^{k} a_i 10^i \pmod{5^{k+1}}$$

As required. Hence such x exists for all $k \geq 1$ by induction. For any k, from (1) and the above result we have shown that there exist $x, y \in \mathbb{Z}$ with

$$x^2 \equiv \sum_{i=0}^{k-1} a_i 10^i \pmod{2^k}$$
$$y^2 \equiv \sum_{i=0}^{k-1} a_i 10^i \pmod{5^k}$$

As before, choosing $z \in \mathbb{Z}$ with $z \equiv x \pmod{2^k}$ and $z \equiv y \pmod{5^k}$ gives $z^2 \equiv \sum_{i=0}^{k-1} a_i 10^i \pmod{10^k}$. Hence $A \in X$ as required.

Referring to the parts of the original question, we let $A = \{1, 4\}$. (i) has been shown above. We can see (ii) using the above method as follows: We know that $12^2 \equiv 144 \pmod{8}$. Extending to (mod 16) as in the above proof with $A = \{1, 4\}$ gives

$$12^2 \equiv 4144 \pmod{16}$$

Now we apply the (very inefficient) algorithm in the above proof to give

$$2^2 \equiv 4 \pmod{5}$$
$$362^2 \equiv 44 \pmod{25} \text{ since } l = 8, m = 3$$
$$(-1177738)^2 \equiv 144 \pmod{125} \text{ since } l = -5236, m = 3$$
$$(-12483602310238)^2 \equiv 4144 \pmod{625} \text{ since } l = -11096534340, m = 3$$

Note that $-12483602310238 \equiv 387 \pmod{625}$. Thus we wish to find $z \in \mathbb{Z}$ with $z \equiv 12 \pmod{16}$ and $z \equiv 387 \pmod{625}$. We have $387 \equiv 3 \pmod{16}$ and $625 \equiv 1 \pmod{16}$, so one such z is $z = 387 + 9 \times 625 = 6012$. Indeed $6012^2 = 36144144$ (in fact $1012^2 = 1024144$ would have sufficed).

(iii) We have $A \cap S = \{1, 4\} \neq \emptyset$, $A \cap E = \{4\} \neq \emptyset$, $|A| = 2 \geq 2$, $1 \in A \setminus \{2, 6, 8\}$ and $1 \in A \setminus \{3, 5, 7, 8\}$. Hence A satisfies the 5 conditions, so $A \in X$. That is, for $k \geq 1$ there exists $x \in \mathbb{Z}$ with the last k digits of x^2 in A.

(iv) Applying the above criteria to each pair, the elements of X with order 2 are

$$\{0,1\},\{0,2\},\{0,3\},\{0,4\},\{0,5\},\{0,6\},\{0,7\},\{0,8\},\{0,9\},$$
$$\{1,2\},\{1,4\},\{1,6\},\{1,8\},\{2,4\},\{2,5\},\{2,9\},\{3,4\},\{3,6\},$$
$$\{4,5\},\{4,6\},\{4,7\},\{4,8\},\{4,9\},\{5,6\},\{6,7\},\{6,9\},\{8,9\}.$$

2. Recall that the Fibonacci numbers $(f_n)_{n\geq 1}$ are defined by $f_1 = f_2 = 1$ and $f_{n+2} = f_{n+1} + f_n$ if $n \geq 1$.

(a) Let $\ell_n \in \{0, 1, \ldots, 9\}$ be the last digit in f_n. Thus the sequence (ℓ_n) starts

$$1, 1, 2, 3, 5, 8, 3, 1, 4, 5, 9, \ldots.$$

Show that this sequence is periodic. What is its period?

(b) Notice that there are 6 n's such that f_n is only one digit long. Show that if $k \geq 2$, there are either 4 or 5 n's such that f_n has exactly k digits.

Solution. (a) The numbers ℓ_n satisfy $\ell_n \equiv f_n \pmod{10}$, and so $\ell_{n+2} \equiv \ell_{n+1}+\ell_n \pmod{10}$. If $(\ell_n, \ell_{n+1}) = (\ell_{n+r}, \ell_{n+r+1}) \pmod{10}$ for some $n \in \mathbb{N}$, then $\ell_{n+r+2} \equiv \ell_{n+r+1} + \ell_{n+r} \equiv \ell_{n+1} + \ell_n \equiv \ell_{n+2}$, and so $(\ell_{n+1}, \ell_{n+2}) = (\ell_{n+r+1}, \ell_{n+r+2}) \pmod{10}$. Similarly, $\ell_{n+r-1} \equiv \ell_{n+r+1} - \ell_{n+r} \equiv \ell_{n+1} - \ell_n \equiv \ell_{n-1}$ and so $(\ell_{n-1}, \ell_n) = (\ell_{n+r-1}, \ell_{n+r}) \pmod{10}$.

A routine induction now shows that $(\ell_m, \ell_{m+1}) = (\ell_{m+r}, \ell_{m+r+1}) \pmod{10}$ for all $m \in \mathbb{N}$, so that $\ell_{m+r} = \ell_m$ for all $m \in \mathbb{N}$. So to show that the sequence (ℓ_n) is periodic, it is enough to find $n, r \in \mathbb{N}$ with $r > 0$ such that $(\ell_n, \ell_{n+1}) = (\ell_{n+r}, \ell_{n+r+1}) \pmod{10}$. This must be possible, because $(\ell_n, \ell_{n+1}) \in \{0, 1, \ldots, 9\}^2$, and so there are at most 100 different possibilities for (ℓ_n, ℓ_{n+1}). A routine calculation shows that $(\ell_r, \ell_{r+1}) = (\ell_0, \ell_1) \pmod{10}$ for $r = 60$, but for no smaller $r > 0$. It follows that the sequence (ℓ_n) is periodic, with period 60.

(b) An integer a is k digits long if and only if $10^{k-1} \leq a < 10^k$. Suppose that $k \geq 2$ and that m is the smallest positive integer such that f_m is k digits long. Then $f_{m-1} < 10^{k-1} \leq f_m < 10^k$. Now $f_{m-1} > f_{m-2}$, and so $f_m = f_{m-1} + f_{m-2} < 2f_{m-1}$. Hence $f_{m-1} > \frac{1}{2} f_m \geq 5 \cdot 10^{k-2}$. Also,

$$\begin{aligned}
f_{m+1} &= f_m + f_{m-1} > 10 \cdot 10^{k-2} + 5 \cdot 10^{k-2} = 15 \cdot 10^{k-2},\\
f_{m+2} &= f_{m+1} + f_m > 15 \cdot 10^{k-2} + 10 \cdot 10^{k-2} = 25 \cdot 10^{k-2},\\
f_{m+3} &= f_{m+2} + f_{m+1} > 25 \cdot 10^{k-2} + 15 \cdot 10^{k-2} = 40 \cdot 10^{k-2},\\
f_{m+4} &= f_{m+3} + f_{m+2} > 40 \cdot 10^{k-2} + 25 \cdot 10^{k-2} = 65 \cdot 10^{k-2},\\
f_{m+5} &= f_{m+4} + f_{m+3} > 65 \cdot 10^{k-2} + 40 \cdot 10^{k-2} = 105 \cdot 10^{k-2} > 10^k.
\end{aligned}$$

Hence f_{m+5} needs at least $k+1$ digits. On the other hand, $f_m = f_{m-1} + f_{m-2} < 2f_{m-1} < 2 \cdot 10^{k-1}$, and so

$$\begin{aligned}
f_{m+1} &= f_m + f_{m-1} < 2 \cdot 10^{k-1} + 10^{k-1} = 3 \cdot 10^{k-1},\\
f_{m+2} &= f_{m+1} + f_m < 3 \cdot 10^{k-1} + 2 \cdot 10^{k-1} = 5 \cdot 10^{k-1},\\
f_{m+3} &= f_{m+2} + f_{m+1} < 5 \cdot 10^{k-1} + 3 \cdot 10^{k-1} = 8 \cdot 10^{k-1} < 10^k.
\end{aligned}$$

Hence f_{m+3} needs at most k digits. So at least the 4 Fibonacci numbers f_m, f_{m+1}, f_{m+2} and f_{m+3} have exactly k digits. The next number, f_{m+4} may or may not have k digits, but f_{m+5} definitely has at least $k+1$ digits (in fact, exactly $k+1$ digits, because one similarly finds that $f_{m+4} < 13 \cdot 10^{k-1}$ and then that $f_{m+5} < 21 \cdot 10^{k-1} < 10^{k+1}$).

3. Oscar and Nicole are playing the following game with matchsticks: They form two piles of matches, one with 42 matches, and the other with 86. They take turns removing matches from the piles, according to the following rule: at each stage the matches taken must all come from one pile, and the number taken must be a divisor of the number of matches in the other pile. The player who removes the last match wins. Nicole goes first. Describe a strategy for Oscar to adopt so that he wins the game, no matter what Nicole does. Show that if we instead start with piles of 40 and 86 matches, the Nicole can always win, if she adopts the correct strategy.

Solution. Let $\mathrm{ord}_2(k)$ denote the number of times 2 divides the integer k.

Step 1. Suppose that at a certain point in the game there are m matches on one pile and n on the other, with $\mathrm{ord}_2(m) = \mathrm{ord}_2(n)$, and that it is Nicole's turn. Then after her move, the numbers m' and n' on the piles will satisfy $\mathrm{ord}_2(m') \neq \mathrm{ord}_2(n')$. For suppose that Nicole removes r matches from the pile of m. Then by the rule, r divides n, and we have $m' = m - r$ and $n' = n$. Let $v = \mathrm{ord}_2(m) = \mathrm{ord}_2(n)$, and write $m = 2^v m_1$ and $n = 2^v n_1$, where m_1 and n_1 are odd. Since r divides n, we have $\mathrm{ord}_2(r) \leq v$. If $\mathrm{ord}_2(r) = v$, write $r = 2^v r_1$, where r_1 is odd. Then $m' = 2^v m_1 - 2^v r_1 = 2^v(m_1 - r_1)$, which is divisible by 2 at least $v+1$ times, because m_1 and r_1 are both odd, forcing $m_1 - r_1$ to be even. Thus $\mathrm{ord}_2(m') \geq v+1 > \mathrm{ord}_2(n')$. If however $\mathrm{ord}_2(r) = u < v$, write $r = 2^u r_1$, with r_1 odd. Then $m' = 2^v m_1 - 2^u r_1 = 2^u(2^{v-u} m_1 - r_1)$ is divisible by 2 exactly u times, because $2^{v-u} m_1 - r_1$ is odd. Thus $\mathrm{ord}_2(m') = u < v = \mathrm{ord}_2(n')$.

Step 2. Suppose that at a certain point in the game there are m matches on one pile and n on the other, with $\mathrm{ord}_2(m) \neq \mathrm{ord}_2(n)$, and that it is Oscar's turn. Then he can choose his move so that the numbers m' and n' on the new piles will satisfy $\mathrm{ord}_2(m') = \mathrm{ord}_2(n')$. For suppose that $m = 2^u m_1$ and $n = 2^v n_1$, where $u < v$ (say) and m_1 and n_1 are odd. Oscar should remove 2^u matches from the pile with n matches. Then $m' = m$ and $n' = n - 2^u = 2^v n_1 - 2^u = 2^u(2^{v-u} n_1 - 1)$ satisfy $\mathrm{ord}_2(m') = \mathrm{ord}_2(n') = u$.

Notice that game starts with $\mathrm{ord}_2(42) = \mathrm{ord}_2(86) = 1$. By Step 1, after Nicole's first move the numbers m and n of matches satisfy $\mathrm{ord}_2(m) \neq \mathrm{ord}_2(n)$. Oscar then makes a move to obtain numbers m' and n' of matches in the piles satisfying $\mathrm{ord}_2(m') = \mathrm{ord}_2(n')$, as he can, by Step 2. Continuing in this way, after any of Nicole's moves we have numbers m and n of matches satisfy $\mathrm{ord}_2(m) \neq \mathrm{ord}_2(n)$. In particular, $m = n = 0$ cannot happen, and so Nicole cannot make the last move.

If instead we start with piles of 40 and 86, then Nicole's first move should be to remove 2 matches from the pile with 40. Then it is as if we started with 38 matches and 86, but with Oscar going first. Since $\mathrm{ord}_2(38) = \mathrm{ord}_2(86) = 1$, Nicole will win if she adopts the strategy described for Oscar in the original game.

4. Let G be a finite group. If $x \in G$, then the conjugacy class of x is the set of elements of the form gxg^{-1}, where $g \in G$. Now suppose that H is a subgroup of G which contains an element from each conjugacy class in G. Show that $H = G$.

Solution. Let $x \in G$. Then H contains an element gxg^{-1} for some $g \in G$. That is, there exist $g \in G$ and $h \in H$ so that $gxg^{-1} = h$. Hence $x = g^{-1}hg$ is an element of the subgroup $g^{-1}Hg = \{g^{-1}hg : h \in H\}$. So our hypothesis tells us that every element x of G belongs to one of the subgroups $g^{-1}Hg$. That is

$$G = \bigcup_{g \in G} g^{-1}Hg. \tag{1}$$

Now let $N = \{g \in G : g^{-1}Hg = H\}$. Then N is a subgroup of G, called the normalizer of H. Clearly $H \subset N$. Suppose that $g_1, g_2 \in G$ and $g_1^{-1}Hg_1 = g_2^{-1}Hg_2$. Then $g_1 g_2^{-1} \in N$.

So the cosets Ng_1 and Ng_2 are equal. Conversely, if $Ng_1 = Ng_2$, then $g_1^{-1}Hg_1 = g_2^{-1}Hg_2$. This means that the number of distinct subgroups $g^{-1}Hg$, as g varies, is the same as the number c of distinct cosets of N in G. Since G is the disjoint union of the distinct cosets Ng, and all these cosets have exactly $|N|$ elements, we have $c = |G|/|N|$.

So there are exactly $c = |G|/|N|$ distinct subgroups $g^{-1}Hg$, say $g_1^{-1}Hg_1, \ldots, g_c^{-1}Hg_c$. Each of these subgroups contains the element 1. So the union on the right in (1) is

$$\{1\} \cup \bigcup_{i=1}^{c} \big(g_i^{-1}Hg_i \setminus \{1\}\big),$$

and it therefore has at most $1+c(|H|-1)$ elements. So (1) implies that $|G| \leq 1+c(|H|-1)$. But $H \subset N$ implies that $c \leq |G|/|H|$, and so $c|H| \leq |G|$. Therefore $|G| \leq 1 + |G| - c$. So $c = 1$. But then $|G| \leq 1 + c(|H| - 1) = |H|$, and so $H = G$.

5. If u and v are distinct roots of the quadratic equation $x^2 - px + q = 0$, then we have $u+v = p$ and $uv = q$. Now suppose that P, Q, U and V are 2×2 matrices and that U and V are distinct solutions of the matrix equation $X^2 - PX + Q = 0$. For a square matrix A, let $\mathrm{Tr}(A)$ denote the sum of its diagonal terms, and let $\det(A)$ denote its determinant. Show that $\mathrm{Tr}(U+V) = \mathrm{Tr}(P)$ and $\det(UV) = \det(Q)$ is true if we add the extra hypothesis that $U - V$ is invertible.

Solution. The result is in fact true for $n \times n$ matrices, for any n. Subtracting the two equations, we have $U^2 - V^2 - P(U - V) = 0$, and so $P = (U^2 - V^2)(U - V)^{-1}$. Let $V' = (U - V)V(U - V)^{-1}$. Then

$$U + V' = \big(U(U - V) + UV - V^2\big)(U - V)^{-1} = (U^2 - V^2)(U - V)^{-1} = P$$

Now $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$, and so $\mathrm{Tr}(V') = \mathrm{Tr}(V)$, and

$$\mathrm{Tr}(U + V) = \mathrm{Tr}(U) + \mathrm{Tr}(V) = \mathrm{Tr}(U) + \mathrm{Tr}(V') = \mathrm{Tr}(U + V') = \mathrm{Tr}(P).$$

Also,

$$\begin{aligned} Q = PU - U^2 = (U^2 - V^2)(U - V)^{-1}U - U^2 &= \big(U^2 - V^2 - U(U - V)\big)(U - V)^{-1}U \\ &= (U - V)V(U - V)^{-1}U. \end{aligned}$$

Since $\det(AB) = \det(A)\det(B)$ for $n \times n$ matrices, we have

$$\det(Q) = \det((U - V)V(U - V)^{-1}U) = \det(V)\det(U) = \det(UV).$$

To see that the result is false without the extra hypothesis that $U - V$ is invertible, choose any quadratic equation $x^2 - px + q = 0$ with two distinct roots u and v. For example, we could take $p = 1$ and $q = 0$, so that $u = 0$ and $v = 1$. Now let

$$P = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}, \quad Q = \begin{pmatrix} q & 0 \\ 0 & q \end{pmatrix}, \quad U = \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} u & 0 \\ 0 & v \end{pmatrix}.$$

Then $\mathrm{Tr}(U + V) = 3u + v$, whereas $\mathrm{Tr}(P) = 2p = 2(u + v)$.

6. Suppose that we have a curve C given by an equation in polar coordinates $r = f(\theta)$, $0 \leq \theta \leq 2\pi$. Here f is a continuous function, and $f(\theta) \geq 0$ for all θ. Assume that the region bounded by this curve is convex. Now consider a segment of length $a + b$, and a point P at distance a from one end of the segment. Imagine sliding this segment round

inside the curve so that its ends are touching C. The point P traces a curve C' inside C. What is the area of the region between the two curves?

Solution. The answer is πab. Here is one solution.

Let X and Y be the ends of the segment. Notice that $f(\theta)$ represents the distance from the origin to X when OX makes an angle of θ with the positive x-axis. Let $g(\theta)$ and $h(\theta)$ denote the distances from O to Y and from O to P, respectively.

The area bounded by C is

$$A = \int_0^{2\pi} \int_0^{f(\theta)} r \, dr \, d\theta = \frac{1}{2} \int_0^{2\pi} f(\theta)^2 \, d\theta.$$

In the same way, A is also equal to $\frac{1}{2}\int_0^{2\pi} g(\theta)^2 \, d\theta$, while the area bounded by C' is $A' = \frac{1}{2}\int_0^{2\pi} h(\theta)^2 \, d\theta$.

Let α denote the angle OXY. Then using the cosine rule for the triangles $\triangle OXY$ and $\triangle OXP$, we get two formulas for $\cos\alpha$:

$$\cos\alpha = \frac{(a+b)^2 + f(\theta)^2 - g(\theta)^2}{2(a+b)f(\theta)} \quad \text{and} \quad \cos\alpha = \frac{a^2 + f(\theta)^2 - h(\theta)^2}{2af(\theta)}.$$

Equating these formulas, multiplying through by $f(\theta)$, and integrating both sides from $\theta = 0$ to $\theta = 2\pi$, the answer drops out, in view of the formulas for A and A' derived above.

7. Suppose that f, c are integers such that $1 \le f \le c$. Under what conditions is it possible to find integers n, m so that $1 \le m < c$ and $(f-1)/c < n/m \le f/c$?

Solution. If $f \ne 1$, then taking $n = f - 1$ and $m = c - 1$, it is easy to check that $(f-1)/c < n/m \le f/c$. If $f = 1$, it is not possible to find n and m, because we want $0 < n/m \le 1/c$ and $m < c$. This would imply that $nc \le m < c$, so that $n < 1$. But then $0 < n/m$ is not true.

8. We consider strings of 0's and 1's, and modify them using the "substitution" rule $\sigma(0) = 01$, $\sigma(1) = 0$ as follows: if $\xi = x_1 x_2 \cdots x_n$ is a string of 0's and 1's, we define $\sigma(\xi)$ to be the concatenation $\sigma(x_1)\sigma(x_2)\cdots\sigma(x_n)$. For example, starting from the string 0, and applying σ repeatedly, we get

$$\sigma(0) = 01, \ \sigma^2(0) = \sigma(01) = 010, \ \sigma^3(0) = \sigma(010) = 01001, \ \text{etc.}$$

(a) Show that $\sigma^n(0)$ is a string of length f_{n+1}, where f_n is the n-th Fibonacci number (see Question 2).

(b) Show that the first f_n letters of $\sigma^n(0)$ are those of $\sigma^{n-1}(0)$.

Because of (b), there is a unique infinite string $\xi = 0100101\cdots$ of 0's and 1's with the property that, for each $n \ge 1$, the first f_n letters of ξ are those of $\sigma^{n-1}(0)$. Notice that the string 11 doesn't appear in ξ, but 00, 01 and 10 do occur. Show that more generally,

(c) For each $n \ge 1$, there are exactly $n+1$ different strings of length n occurring somewhere in ξ.

Solution. Let $\xi_n = \sigma^n(0)$ for $n = 0, 1, \ldots$. We first show that, for $n = 0, 1, \ldots$,

$$\xi_{n+2} = \xi_{n+1}\xi_n. \tag{1}$$

Firstly, $\xi_0 = 0$, $\xi_1 = 01$, and $\xi_1\xi_0 = 010 = \xi_2$, so that (1) holds for $n = 0$. Now suppose that (1) holds for $n = m - 1$ for some $m \ge 1$. Then

$$\xi_{m+2} = \sigma^{m+2}(0) = \sigma(\sigma^{m+1}(0)) = \sigma(\xi_{m+1}) = \sigma(\xi_m\xi_{m-1}) = \sigma(\xi_m)\sigma(\xi_{m-1}) = \xi_{m+1}\xi_m,$$

so that (1) holds for $n = m$.

We can now prove (a) and (b). For if ℓ_n denotes the length of ξ_n, then (1) shows that $\ell_{n+2} = \ell_{n+1} + \ell_n$, and since $\ell_0 = 1 = f_1$ and $\ell_1 = 2 = f_2$, an obvious induction shows that $\ell_n = f_{n+1}$ for each $n \geq 0$, so that (a) holds. By (1), we have $\xi_n = \xi_{n-1}\xi_{n-2}$, and since ξ_{n-1} has length f_n by (a), the first f_n letters of $\sigma^n(0) = \xi_n$ are the letters of $\xi_{n-1} = \sigma^{n-1}(0)$.

The proof of (c) involves a number of steps.

(i) We can define the action of σ on infinite strings of 0's and 1's in the obvious way. Let us next show that $\sigma(\xi) = \xi$. For let $n \geq 0$ be an integer. Then the first f_{n+1} letters of ξ are those of ξ_n, and so the first f_{n+2} letters of $\sigma(\xi)$ are those of $\sigma(\xi_n) = \xi_{n+1} = \xi_n\xi_{n-1}$. Thus the first f_{n+1} letters of $\sigma(\xi)$ are those of ξ_n, and hence those of ξ. Hence $\sigma(\xi)$ and ξ agree in their first f_{n+1} letters. Since $n \geq 1$ was arbitrary, and $f_n \to \infty$ as $n \to \infty$, we see that $\sigma(\xi) = \xi$.

(ii) Let us next show that the strings 11, 000 and 10101 do not appear in ξ. To exclude 11 is easy, but the following method can be used for the other two cases. Suppose that the letters of ξ are x_1, x_2, $x_3, \ldots$. Then $\xi = \sigma(\xi) = y_1y_2y_3\cdots$, where

$$y_i = \begin{cases} 01 & \text{if } x_i = 0, \\ 0 & \text{if } x_i = 1. \end{cases}$$

So if a 1 appears in ξ, then it appears in one of the y_i's, and so is preceded by a 0. Hence 11 does not appear in ξ.

Now suppose that 000 appears in ξ. Then if the first of these 0's appears in y_i, then the string 000 appears in $y_iy_{i+1}y_{i+2}$, since each y_j has length at least 1. The possible $y_iy_{i+1}y_{i+2}$'s, are

$$010101,\ 01010,\ 01001,\ 00101,\ \text{and } 0010, \tag{2}$$

according as $x_ix_{i+1}x_{i+2} = 000$, 001, 010, 100 or 101 (the strings 011, 110 and 111 being excluded as possible $x_ix_{i+1}x_{i+2}$'s, since 11 does not appear in ξ). We observe that 000 does not appear in any of the strings (2).

We can exclude 10101 similarly. If it appears in ξ, then it appears in $y_iy_{i+1}y_{i+2}y_{i+3}y_{i+4}$ for some i. Of the 32 strings of 5 0's and 1's, all but 7 are excluded as possibilities for $x_ix_{i+1}x_{i+2}x_{i+3}x_{i+4}$'s since 11 and 000 do not appear in ξ. The non-excluded 7 are

$$00100,\ 00101,\ 01001,\ 01010,\ 10010, 10100,\ \text{and } 10101.$$

and one may quickly check that none of the corresponding $y_iy_{i+1}y_{i+2}y_{i+3}y_{i+4}$'s contains 10101.

(iii) Let us next show that if $s = x_1\cdots x_k$ and $s' = x'_1\cdots x'_\ell$ are two finite strings of 0's and 1's, and if $\sigma(s) = \sigma(x_1)\cdots\sigma(x_k)$ equals $\sigma(s') = \sigma(x'_1)\cdots\sigma(x'_\ell)$, then $s = s'$. We prove this by induction on $\min\{k, \ell\}$. If $k = 0$, say, then s is empty, so that $\sigma(s)$ is empty, and so $\sigma(s')$ and s' must be empty too. Now assume that $k, \ell \geq 1$. If $x_k \neq x'_\ell$, then we may assume that $x_k = 0$ and $x'_\ell = 1$. But then $\sigma(s)$ ends in a 1 and $\sigma(s')$ ends in a 0, contrary to our hypothesis. Hence $x_k = x'_\ell$. Now by applying the induction hypothesis to the shorter strings $x_1\cdots x_{k-1}$ and $x'_1\cdots x'_{\ell-1}$, we see that $s = s'$.

(iv) Let us now show that there is no string v of 0's and 1's such that both $0v0$ and $1v1$ appear in ξ. We prove this by induction on the length $\ell(v)$ of v. Suppose that v is a string of minimal length such that both $0v0$ and $1v1$ appear in ξ. Firstly, v is not the empty string, and it neither begins nor ends in 1 because 11 does not appear in ξ. Similarly, v is not simply 0, because 000 does not appear in ξ. Hence $v = 0w0$ for some string w. So the string $00w00$ appears in ξ, and so is in a finite string $y_iy_{i+1}\cdots y_{i+r-1}$ of length r, say, for some i such that the first 0 of $00w00$ is in y_i. By considering the three possibilities

00, 01 and 10 for $x_i x_{i+1}$, the only way to get the first 00 in $00w00$ is if $x_i x_{i+1} = 10$. Similarly, by considering the final 00 in $00w00$, we see that a string $10h10$ must appear in ξ, so that $\sigma(10h10) = 00w001$. We have $\sigma(0h) = 0w$ and $\sigma(10h1) = 00w0$. Let $x = 0h$. Then $1x1$ appears in ξ and $\sigma(1x1) = 00w0$. Now $1v1 = 10w01$ also appears in ξ, and therefore $010w01$ does too, since ξ does not start with 1. A similar analyis shows that $010w01 = \sigma(0x'0)$ for some string x' such that $0x'0$ is in ξ and $\sigma(x') = 0w$. By step (v), we must have $x' = x$. Thus both $0x0$ and $1x1$ appear in ξ. Since $\sigma(x) = 0w$, we see that $\ell(x) \leq \ell(\sigma(x)) = \ell(w) + 1 = \ell(v) - 1$. This contradict the minimality of $\ell(v)$.

(v) We can now show that for each $n \geq 1$, there are exactly $n + 1$ distinct strings of 0's and 1's of length n which appear in ξ. This is clearly true if $n = 1$, and so we suppose that $m \geq 1$ and that the result holds for $n = m$. Let $s_1, \ldots, s_{m+1}$ be the distinct strings of length m which appear in ξ. For each j, either $0s_j$ or $1s_j$ appears in ξ. For there must be an n such that s_j is a substring of ξ_n. If s_j does not start at the beginning of ξ_n, then ϵs_j appears in ξ_n and hence in ξ, where ϵ is the letter of ξ_n immediately before the start of s_j. If s_j does start at the beginning of ξ_n, then notice that s_j is also a substring of $\xi_{n+1}\xi_n = \xi_{n+2}$, and all of ξ_{n+1} is to the left of s_j. So either $0s_j$ or $1s_j$ appears in ξ_{n+2} and hence in ξ.

If ϵs_j and δs_k appear in ξ, where $\epsilon, \delta \in \{0, 1\}$ and $j \neq k$, then clearly $\epsilon s_j \neq \delta s_k$. So we have at least $m + 1$ different strings of length $m + 1$ in ξ. Moreover, any string of length $m + 1$ in ξ must have the form ϵs_j for $\epsilon = 0$ or 1, and for some $j \in \{1, \ldots, m + 1\}$. So to complete the induction step, it is enough to show that there is exactly one string s of 0's and 1's having length m and such that both $0s$ and $1s$ appear in ξ.

Firstly, there is such a string s. For choose n so large that $f_{n+1} \geq m$, and let s be the beginning m letters of ξ_n. Since ξ_{n+1} starts with ξ_n, we see that s is also the beginning m letters of ξ_{n+1}. If n is even, then ξ_{n+1} ends in a 1, and so $\xi_{n+1}\xi_n = \xi_{n+2}$ contains the string $1s$. If n is odd, then ξ_{n+2} ends in an 0, and so $\xi_{n+2}\xi_{n+1} = \xi_{n+3}$ contains the string $0s$. So both $0s$ and $1s$ appear in ξ.

Suppose that there are two distinct strings s and s' of length m such that $0s$, $1s$, $0s'$ and $1s'$ all appear in ξ. Consider the first letter of s (reading from the left) which does not equal the corresponding letter of s'. We may assume that this letter is 0 in s and 1 in s'. Let v denote the (possibly empty) part of s and s' preceding these differing letters. Then $0v0$ is a substring of $0s$ and so appears in ξ. Similarly, $1v1$ is a substring of $1s'$ and so appears in ξ. This contradicts step (iv) above, and therefore the induction step, and so the proof of (c), is complete.

9. We consider a fixed finite alphabet of *symbols* and strings of these symbols. The strings have a fixed length n, and a string of length n will be called a *word*. We think of the symbols in a word as occurring in n places, so we can talk about the symbol in the first place in a word, the symbol in the second place, and so forth.

We define the *(Hamming) distance* between two words to be the number of places in which they differ.

Consider functions from the set of all words to itself which preserve the Hamming distance. Here are two examples of such functions.

(i) Apply a permutation to the places. For example if $n = 3$ and we swap the first two places, the word *abc* will be changed into the word *bac*.

(ii) Apply a permutation to the symbols in one place. For example, in the first place we might change a to b, b to c and c to a. The word *abc* would be changed into *bbc*.

Show that every function from the set of all words to itself which preserves the Hamming distance is a composite of functions of types (i) and (ii) above.

Solution. Let us first make some preliminary comments. As usual, we denote the composite two functions ψ, ϕ by $\psi \circ \phi$, i.e., $(\psi \circ \phi)(w) = \psi(\phi(w))$. We write $d(u, v)$ for the

(Hamming) distance between u and v. Let Σ denote the alphabet, and let W denote the set of all words of length n over Σ. A function $f : W \to W$ which preserves distance must be a bijection; to see that f is 1–1, note that $u \neq v$ implies $d(u, v) > 0$ so that $d(\phi(u), \phi(v)) > 0$, which implies that $\phi(u) \neq \phi(v)$. This is all we need to check, since a 1–1 function from a finite set to itself is a bijection. It is clear that the inverse of a distance-preserving function is also distance-preserving. Also, the inverse of a function of type (i) in the problem statement is again of type (i), and the same is true for functions of type (ii).

If Σ has only one element, then $|W| = 1$, and there is nothing to prove. So assume that $|\Sigma| \geq 2$. We may as well assume that two of the elements of Σ are 0 and 1.

For each $i \in \Sigma$, let $\mathbf{i}$ denote the string $ii \cdots i$ of length n. Then $d(\mathbf{i}, \mathbf{j}) = n$ for each $i \neq j$. Hence $d(f(\mathbf{i}), f(\mathbf{j})) = n$ if $i \neq j$. This means that for $\nu = 1, \ldots, n$, the ν-th symbol $f(\mathbf{i})_\nu$ in $f(\mathbf{i})$ is different from the ν-th symbol $f(\mathbf{j})_\nu$ in $f(\mathbf{j})$. So for each fixed ν, the map $\pi_\nu : i \mapsto f(\mathbf{i})_\nu$ is 1–1 on Σ, and is therefore a bijection. Let g denote the map $W \to W$ defined by

$$g(x_1 x_2 \cdots x_n) = \pi_1(x_1)\pi_2(x_2) \cdots \pi_n(x_n).$$

Then g is a composition of n maps of the form (ii). Moreover,

$$f(\mathbf{i}) = g(\mathbf{i}) \quad \text{for each } i \in \Sigma.$$

Replacing f by $g^{-1} \circ f$, we may assume that $f(\mathbf{i}) = \mathbf{i}$ for each $i \in \Sigma$.

Notice that for any $x = x_1 x_2 \cdots x_n \in W$, $n - d(x, \mathbf{i})$ is the number of j's such that $x_j = i$, i.e., the number of occurrences of the letter i in the string x. Now that we are assuming that $f(\mathbf{i}) = \mathbf{i}$ for each $i \in \Sigma$, we know that x and $f(x)$ have the same number of i's, for each $i \in \Sigma$.

Let w_j denote the string of length n having a 1 in position j and all other symbols 0. By the preceding paragraph, we know that $f(w_j)$ has $n-1$ 0's and one 1. Hence $f(w_j) = w_k$ for some $k \in \{1, \ldots, n\}$. If $j \neq j'$, and $f(w_j) = w_k$ and $f(w_{j'}) = w_{k'}$, then $w_j \neq w_{j'}$ and so $w_k \neq w_{k'}$. So the map $j \mapsto k$ is a 1–1 function on Σ. Let us denote this map by σ. That is, $f(w_j) = w_{\sigma(j)}$ for each j. Since the map $j \mapsto \sigma(j)$ is a 1–1 map from $\{1, \ldots, n\}$ to itself, it is a bijection, i.e., a permutation of $\{1, \ldots, n\}$.

The map $g : W \to W$ defined by

$$g(x_1 x_2 \cdots x_n) = x_{\sigma^{-1}(1)} x_{\sigma^{-1}(2)} \cdots x_{\sigma^{-1}(n)}$$

is a map of the form (i), and so preserves that Hamming distance. Moreover $g(\mathbf{i}) = \mathbf{i}$ for each $i \in \Sigma$, and $g(w_j) = w_{\sigma(j)} = f(w_j)$ for $j = 1, \ldots, n$. Hence, replacing f by $g^{-1} \circ f$, we may assume that $\sigma = id$. In other words, we may assume that f fixes all the words w_j, $j = 1, \ldots, n$, as well as the words $\mathbf{i}$, $i \in \Sigma$. We now show that f must be the identity map. We show that $f(x) = x$ for each $x = x_1 \cdots x_n \in W$ by induction on the number of j's such that $x_j \neq 0$.

Let's first show that $f(x) = x$ if x has only one nonzero letter. If this letter is 1, then we are done, because $x = w_j$ for some j. So suppose that $x_j = a \neq 0, 1$, and that all other letters of x are 0. Then $f(x)$ is a string containing one a and all other letters 0. Suppose that this a occurs in position j'. If $j' \neq j$, then $d(f(x), w_j) = 2$, whereas $f(x, w_j) = 1$. So $j' = j$, which means that $f(x) = x$.

Now suppose that $x = x_1 \cdots x_n$ has exactly $k > 1$ letters which are nonzero, and that we have shown that $f(x') = x'$ for all strings x' with only $k - 1$ nonzero letters. Pick some j so that $x_j = a \neq 0$. Let x' be the string which equals x except that its j-th letter is 0. Then by assumption, $f(x') = x'$. Also, let x'' be the string whose j-th letter is a and all of whose other letters are 0. We know that $f(x'') = x''$ too. Also, $d(x, x') = 1$ and

$d(x, x'') = k - 1$ (since x and x'' have exactly $n - k$ 0's in common, and also agree at the j-th letter. Now $d(f(x), x') = d(f(x), f(x')) = d(x, x') = 1$, and $f(x)$ has exactly $n - k$ 0's, whereas x' has $n - k + 1$ 0's. So $f(x)$ must be obtained from x' by replacing one of x''s 0's by a nonzero letter. This letter must be a, because $f(x)$ has the same number of a's as x has. Suppose that $f(x)$ is obtained from x' by replacing a 0 in position j' by an a. If we can show that $j' = j$, then $f(x) = x$. If $j' \neq j$, then $f(x)$ has exactly $n - k - 1$ 0's in positions different from j. The j-th letters of $f(x)$ and x'' are 0 and a respectively, so that $f(x)$ and x'' agree in exactly $n - k - 1$ places, so that $d(f(x), x'') = k + 1$. But this contradicts $d(f(x), x'') = d(f(x), f(x'')) = d(x, x'') = k - 1$. Hence $j' = j$, and $f(x) = x$.

10. Let q be a prime power, $\mathbb{F}_q$ the finite field with q elements, and $\alpha \in \mathbb{F}_q$. Let $\mathbb{F}_q[X]$ denote the set of polynomials with coefficients in $\mathbb{F}_q$. A polynomial is called irreducible if it cannot be written as a product of two polynomials both have smaller degree. Each $f \in \mathbb{F}_q[X]$ can be written as a product of irreducible polynomials. For $n \geq 1$, the number of monic polynomials in $\mathbb{F}_q[X]$ of degree n with constant term α is clearly q^{n-1}. How many of these polynomials have distinct irreducible factors?

Solution. (Due to Peter McNamara, University of Sydney.) For $\alpha \in \mathbb{F}_q$, let $f(n, \alpha)$ denote the number of monic polynomials in $\mathbb{F}_q[x]$ of degree n having constant term α and distinct irreducible factors. We shall see that the formula for $f(n, \alpha)$ is a little different depending on whether n is even or odd, and whether α is a square in $\mathbb{F}_q$ or not. There are several steps.

(i) Each monic polynomial $f \in \mathbb{F}_q[x]$ may be written uniquely as $f = gh^2$, where $g, h \in \mathbb{F}_q[x]$ are monic and where g has distinct irreducible factors. To see this, note that f may be written $p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$, where $p_1, \ldots, p_r$ are distinct irreducible monic polynomials and $m_1, \ldots, m_r \geq 1$. Order the p_j's so that the m_i's are odd, $m_i = 2n_i + 1$ say, for $i = 1, \ldots, s$, and the m_i's are even, $m_i = 2n_i$ say, for $i = s + 1, \ldots, r$. Then $f = (p_1 \cdots p_s)(p_1^{n_1} \cdots p_r^{n_r})^2$ is a factorization $f = gh^2$ of the desired type. This factorization is unique, because if $f = gh^2$ with $g = p_1 \cdots p_s$, and the p_j's distinct irreducibles, then write $h = p_1^{n_1} \cdots p_r^{n_r}$, where $n_1, \ldots, n_r \geq 0$ (and $n_{s+1}, \ldots, n_r \geq 1$) and all the p_j's are distinct irreducibles. Then $f = p_1^{2n_1+1} \cdots p_s^{2n_s+1} p_{s+1}^{2n_{s+1}} \cdots p_r^{2n_r}$, and this must be the factorization of f into a product of monic irreducibles, which is unique up to order because $\mathbb{F}_q[x]$ is a unique factorization domain.

(ii) For each $k \geq 1$, the number of monic polynomials $h = x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ of degree k having a nonzero constant term is $q^{k-1}(q - 1)$. This is clear because there are q choices for each of the coefficients $a_1, \ldots, a_{k-1}$, but only $q - 1$ for a_0 since we require that $a_0 \neq 0$.

(iii) The number $f(2n + 1, \alpha)$ is the same for all nonzero $\alpha \in \mathbb{F}_q$. Thus $f(2n + 1, \alpha) = f(2n + 1, 1)$. This is clearly true for $n = 0$, since $x + \alpha$ is the only monic polynomial of degree 1 having constant term α. Now assume that $n > 0$, and assume the result for all smaller n's. Consider the set $\mathcal{S}_{2n+1,\alpha}$ of all monic polynomials of degree $2n + 1$ having constant term α. Clearly there are q^{2n} polynomials in $\mathcal{S}_{2n+1,\alpha}$. Now $\mathcal{S}_{2n+1,\alpha}$ is the disjoint union of the sets $\mathcal{S}_{2n+1,\alpha,k}$, $k = 0, \ldots, n$, where $\mathcal{S}_{2n+1,\alpha,k}$ consists of all the monic polynomials f of degree $2n+1$ having constant term α for which the h in the factorization $f = gh^2$ of step (i) above has degree k. We count the number of polynomials in each $\mathcal{S}_{2n+1,\alpha,k}$. If $k = 0$, then $f = g$, and so $|\mathcal{S}_{2n+1,\alpha,0}| = f(2n + 1, \alpha)$. If $1 \leq k \leq n$, write $h = x^k + b_{k-1}x^{k-1} + \cdots + b_1 x + b_0$ and $g = x^\ell + a_{\ell-1}x^{\ell-1} + \cdots + a_1 x + a_0$. Then $a_0 b_0^2 = \alpha$ must hold. That is, the constant term in g must be $\alpha/h(0)^2$. By Step (ii), there are $q^{k-1}(q - 1)$ choices of h, and for each one, there are $f(2(n - k) + 1, \alpha/h(0)^2)$ choices of g. By the induction hypothesis, we have $f(2(n-k)+1, \alpha/h(0)^2) = f(2(n-k)+1, 1)$. Hence

$|\mathcal{S}_{2n+1,\alpha,k}| = f(2(n-k)+1,1)q^{k-1}(q-1)$, and so

$$q^{2n} = f(2n+1,\alpha) + \sum_{k=1}^{n} f(2(n-k)+1,1)q^{k-1}(q-1), \tag{1}$$

which shows that $f(2n+1,\alpha)$ is independent of the nonzero α.

(iv) We can now show that for each nonzero $\alpha \in \mathbb{F}_q$,

$$f(2n+1,\alpha) = \frac{q^{2n+1}+1}{q+1}.$$

For we can form the generating function $F(x) = \sum_{n=0}^{\infty} f(2n+1,\alpha)x^n$. Multiplying both sides of (1) by x^n, then summing, we get

$$\frac{1}{1-q^2x} = F(x) + \frac{(q-1)x}{1-qx}F(x).$$

Rearranging, we have

$$F(x) = \frac{1}{q+1}\Big(\frac{q}{1-q^2x} + \frac{1}{1-x}\Big),$$

and from this we can read off that the coefficient of x^n is $(q^{2n+1}+1)/(q+1)$.

We now turn to the case of polynomials of even degree, where we still assume that $\alpha \neq 0$. We shall see that the answer depends on whether α is a square in $\mathbb{F}_q$. As is well known, if q is odd, then $(q-1)/2$ elements of $\mathbb{F}_q \setminus \{0\}$ are squares and $(q-1)/2$ are not. If q is even, then all elements of $\mathbb{F}_q$ are squares. If $\alpha \in \mathbb{F}_q$, let s_α denote the number of $x \in \mathbb{F}_q$ such that $x^2 = \alpha$. Thus $s_\alpha = 0$ or 2 if q is odd, and $s_\alpha = 1$ if q is even.

(v) The number $f(2n+2,\alpha)$ depends only on n, q and whether or not α is a square in $\mathbb{F}_q$. As before, we do an induction on n. If $n = 0$, then the polynomials of degree 2 having constant term α which do not have distinct irreducible factors are the polynomials $(x+s)^2 = x^2 + 2sx + s^2$, where s is a square root of α. There are s_α such polynomials. The ones with distinct irreducible factors are the polynomials $x^2 + cx + \alpha$, where $c \neq 2s$ for any square root of α, and so $f(2,\alpha) = q - s_\alpha$. Now assume that $n \geq 1$ and that the result has been proved for polynomials of smaller degree. As in step (iii) above we consider the set $\mathcal{S}_{2n+2,\alpha}$ of all monic polynomials of degree $2n+2$ having constant term α. Clearly $|\mathcal{S}_{2n+2,\alpha}| = q^{2n+1}$. Now $\mathcal{S}_{2n+2,\alpha}$ is the disjoint union of the sets $\mathcal{S}_{2n+2,\alpha,k}$, $k = 0,\ldots,n+1$, where $\mathcal{S}_{2n+2,\alpha,k}$ consists of all the monic polynomials f of degree $2n+2$ having constant term α for which the h in the factorization $f = gh^2$ of step (i) above has degree k. As before, $|\mathcal{S}_{2n+2,\alpha,0}| = f(2n+2,\alpha)$. To count $|\mathcal{S}_{2n+1,\alpha,k}|$ when $k \leq n$, as before there are $q^{k-1}(q-1)$ choices of h, and then g must have constant term $\alpha/h(0)^2$). Since $\alpha/h(0)^2$ is a square if and only if α is, the number $|f(2(n-k)+2,\alpha/h(0)^2)|$ does not depend on the the nonzero number $h(0)$, and so $|\mathcal{S}_{2n+1,\alpha,k}| = f(2(n-k)+2,\alpha)q^{k-1}(q-1)$. The count of $|\mathcal{S}_{2n+1,\alpha,k}|$ is different when $k = n+1$, because g must be 1, and $h(0)$ must satisfy $h(0)^2 = \alpha$. There are clearly $q^n s_\alpha$ monic polynomials h for which $h(0)^2 = \alpha$. Hence we obtain

$$q^{2n+1} = f(2n+2,\alpha) + \sum_{k=1}^{n} f(2(n-k)+2,\alpha)q^{k-1}(q-1) \quad + q^n s_\alpha. \tag{2}$$

(vi) We can now show that for nonzero α,

$$f(2n+2,\alpha) = \frac{q(q^{2n+1}+1)}{q+1} - s_\alpha.$$

Again, form the generating function $F(x) = \sum_{n=0}^{\infty} f(2n+2,\alpha)x^n$. Multiplying both sides of (2) by x^n, then summing, we get

$$\frac{q}{1-q^2x} = F(x) + \frac{(q-1)x}{1-qx}F(x) + \frac{s_\alpha}{1-qx}.$$

Rearranging, we have

$$F(x) = \frac{q}{q+1}\Big(\frac{q}{1-q^2x} + \frac{1}{1-x}\Big) - \frac{s_\alpha}{1-x},$$

and from this we can read off that the coefficient of x^n is $q(q^{2n+1}+1)/(q+1) - s_\alpha$.

(vii) Finally, we deal with the case $\alpha = 0$. A polynomial f of degree n with distinct irreducible factors is just a polynomial $xg(x)$, where g is a polynomial of degree $n-1$ with distinct irreducible factors and nonzero constant term. Hence $f(1,0) = 1$, and

$$f(n,0) = \sum_{\alpha\in\mathbb{F}_q\setminus\{0\}} f(n-1,\alpha) \quad \text{if } n > 1.$$

If n is even, then $n-1$ is odd, and $f(n-1,\alpha) = (q^{n-1}+1)/(q+1)$ for all nonzero α. Thus

$$f(n,0) = \frac{(q-1)(q^{n-1}+1)}{q+1} \quad \text{if } n \text{ is even.}$$

If n is odd, then the result of Step (vi) is that $f(n-1,\alpha) = (q^{n-1}+q)/(q+1) - s_\alpha$ for each α. Summing over the nonzero α, and noticing that $\sum_{\alpha\neq 0} s_\alpha = q-1$, we get

$$f(n,0) = \frac{(q-1)(q^{n-1}+q)}{q+1} - (q-1) = \frac{(q-1)(q^{n-1}-1)}{q+1} \quad \text{if } n > 1 \text{ is odd.}$$