Problemen

| Problem Section

Edition 2006/1

For Session 2006/1 We received submissions from Rik Bos, Thomas Decru, Ruud Jeurissen, Jaap Spies, B. Sury, the Fejéntaláltuka Szeged Problem Solving Group, Peter Vandendriessche, and Gerd Verbouwe.

Problem 2006/1-A We are given a lamp and a sufficiently large number of synchronised time switches that can be turned on or off by the quarter of an hour and have a revolution time of 24 hours. We are going to mount a finite number of switches on top of each other, and put the lamp on top of the result. At the beginning, all time switches are synchronised at 24.00 hours. We define a *period* to be a time span in which the lamp is on for at least one quarter of an hour, and is off for at least one quarter of an hour, and which repeats itself. Which periods, shorter than 4 days, can be constructed?

Solution No solutions were sent in. The solution below is based on that of the proposer Jurjen Bos.
The smallest unit of time is a quarter of an hour. In 24 hours we consider 96 such units, and in 4 days we consider 384 units.
With one switch we are able to create periods of length m units, where m divides 96 and $m > 1$. So with one switch we can create periods of length $2, 3, 4, 6, 8, 12, 16, 24, 32$ and 48 units.
What happens when we combine two switches? Since we are not interested in how long (and in when) the light burns during one period, we may assume the light only burns the first unit of the period.
Suppose a set A of switches causes a period of a units, while a set B causes a period of b units. Assuming that the light burns just 1 unit in each of the periods caused by A and B, we see that the combination of the sets A and B causes a period of ab units.
Notice that the only prime divisors of 96 are 2 and 3. Any combination of switches will increase the factor 2 and/or 3 in the length of the period. The periods we find are therefore:

- 2 switches $9, 18, 36, 64, 72, 128, 144, 192, 256, 288, 384$
- 3 switches $27, 54, 108, 216$
- 4 switches $81, 162, 324$
- 5 switches 243

Problem 2006/1-B Let $P = (0, 0), Q = (3, 4)$. Find all points $A = (X, Y)$ such that

- X and Y are integers,
- the lengths of line segments PA and QA are integers.

Solution This problem was solved by Peter Vandendriessche. The solution below is based on his solution.
We modify the problem a little bit by introducing a coordinate transformation T (a combination of a translation and point-multiplication by a factor 2):

$$\begin{cases} x = 2X - 3 \\ y = 2Y - 4 \end{cases} \qquad \begin{cases} X = \frac{x+3}{2} \\ Y = \frac{y+4}{2} \end{cases}$$

Let $R = T(P) = (-3, -4)$, $S = T(Q) = (3, 4)$ and $B = T(A)$. With the new coordinates the problem is symmetric about $(0, 0)$. Notice that x has to be odd and y has to be even, in order that (X, Y) will be a lattice point. Since the transformation T consist of a multiplication by a factor 2, the distances $\overline{BR}$ en $\overline{BS}$ have to be even, and so does the difference. Let therefore

$$2d = \overline{BR} - \overline{BS} = \sqrt{(x+3)^2 + (y+4)^2} - \sqrt{(x-3)^2 + (y-4)^2}.$$

After squaring this equation, we have

Eindredactie: Matthijs Coster
Redactieadres: Problemenrubriek NAW
Mathematisch Instituut
Postbus 9512
2300 RA Leiden
uwc@nieuwarchief.nl

$$4d^2 = 2x^2 + 2y^2 + 50 - 2\sqrt{(x^2+y^2+25)^2 - (6x+8y)^2}.$$

Dividing by 2 leads to

$$x^2 + y^2 + 25 - 2d^2 = \sqrt{(x^2+y^2+25)^2 - 4(3x+4y)^2}.$$

After squaring (again) and dividing by 4 we have

$$0 = d^4 - d^2(x^2+y^2+25) + (3x+4y)^2. \qquad (*)$$

Notice that $x \equiv 1 \bmod 2$ and $y \equiv 0 \bmod 2$, whence $d \equiv 1 \bmod 2$. Using the triangle inequality we find that $|2d| < 10$. Therefore $|d| \in \{1,3,5\}$.

If $|d| = 5$, $(*)$ can be reduced to $(4x-3y)^2 = 0$. Therefore $(x,y) = (3\lambda, 4\lambda)$, or in terms of the original coordinates, $(X,Y) = (3\mu, 4\mu)$, where μ is integral.

For the case $|d| = 3$, the equality $(*)$ can be reduced to $7y^2 + 24xy = 144$. Substitute $y = 12v$. We find $v(7v+2x) = 1$. There are only 2 integral solutions: $(x,v) = (3,1)$ and $(x,v) = (-3,-1)$. Then $(x,y) = (3,12)$ and $(x,y) = (-3,-12)$, or in terms of the original coordinates $(X,Y) = (3,-4)$ and $(X,Y) = (0,8)$.

Finally, if $|d| = 1$, then $(*)$ can be reduced to $8x^2 + 24xy + 15y^2 = 24$. Substitute $y = 4v$. We find $x^2 + 12xv + 30v^2 = 3$. Now substitute $u = x + 6v$. We have

$$u^2 - 6v^2 = 3. \qquad (**)$$

This equation is a well-known Pell equation, which can be solved using algebraic number theory. The solutions of (**) are of the form (u_n, v_n) where u_n and v_n both satisfy $z_{n+1} = 10z_n - z_{n-1}$. Consequently, the solutions (x,y) of (*) are of the form (x_n, y_n) where x_n and y_n also both satisfy $z_{n+1} = 10z_n - z_{n-1}$. Moreover, the values for $n = 0,1$ are fixed: either $(x_0,y_0) = (-3,4)$ and $(x_1,y_1) = (-39,44)$, or $(x_0,y_0) = (9,-4)$ and $(x_1,y_1) = (93,-44)$. For the solutions (X,Y) of the initial problem, this leads to the recurrences $X_{n+1} = 10X_n - X_{n-1} - 12$ and $Y_{n+1} = 10Y_n - Y_{n-1} - 16$ with initial values $(X_0,Y_0) = (0,4)$, $(X_1,Y_1) = (-18,24)$ or $(X_0,Y_0) = (6,0)$, $(X_1,Y_1) = (48,-20)$.

Problem 2006/1-C Let $n \geq 1$ be an integer and $f(x) = a_n x^n + \cdots + a_0$ be a polynomial with real coefficients. Suppose that f satisfies the following condition:

$$|f(\xi)| \leq 1 \quad \text{for each } \xi \in [-1,1].$$

Consider the polynomial

$$g(x) = a_0 x^n + \cdots + a_n,$$

the reciprocal polynomial of f. Show that g satisfies

$$|g(\xi)| \leq 2^{n-1} \quad \text{for each } \xi \in [-1,1].$$

Solution This problem has been solved by Peter Vandendriessche, Rik Bos, and the Fejéntaláltuka Szeged Problem Solving Group. The solution below is based on that of the proposer.

It is clear, by writing $g(x) = x^n f(1/x)$, that we have to prove that $|a_n| \leq 2^{n-1}$ and $|f(\xi)| \leq 2^{n-1}|\xi|^n$ for all $\xi \in \mathbf{R}$ with $|\xi| > 1$. Furthermore we can assume, without loss of generality, that $a_n > 0$.

Before we start proving the desired properties of f, we recall the definition of the Chebyshev polynomials as well as some identities that they satisfy. Define recursively

$$T_0(x) = 1,\ T_1(x) = x; \quad T_{n+2}(x) = 2xT_{n+1}(x) - T_n(x) \quad \text{for } n \geq 0.$$

The following identities are satisfied by T_n:

$$T_n(\cos\alpha) = \cos n\alpha; \quad T_n(\cosh t) = \cosh nt.$$

Let n be at least 1. From the first identity we see that $|T_n(\xi)| \leq 1$ for all $\xi \in [-1,1]$. From the second identity and the fact that $T_n(-x) = (-1)^n T_n(x)$ it is clear that $|T_n(\xi)| \leq$

$2^{n-1}|\xi|^n$ for all $\xi \in \mathbf{R}$ with $|\xi| > 1$. From the recursion defining T_n we see that the leading coefficient of T_n is equal to 2^{n-1}. So the T_n form an optimal example of polynomials satisfying the conditions and the conclusion of the problem.
First we will prove the following lemma:

Lemma. *Let f be a polynomial with real coefficients satisfying $|f(\xi)| \leq 1$ for all $\xi \in [-1,1]$. Then for each $n \geq 1$, the polynomial $P(x) = f(x) - T_n(x)$ has at least n zeroes on $[-1,1]$, counted with multiplicity.*

Proof. If we put $x_k = \cos\left(\frac{(n-k)\pi}{n}\right)$ for $k \in \{0,\ldots,n\}$, then $-1 = x_0 < x_1 < \cdots < x_n = 1$ and $T_n(x_k) = (-1)^{n-k}$. Furthermore $\frac{d}{dx}T_n(x_k) = 0$ for each $k \neq 0, n$. This means that

$$f(x+x_k) = P(x+x_k) + T(x+x_k) = P(x_k) + T(x_k) + \frac{d}{dx}P(x_k)x + O(x^2). \qquad (1)$$

If $P(x_k) \neq 0 \neq P(x_{k+1})$ then by the intermediate value theorem, P has a zero on (x_k, x_{k+1}). If $P(x_k) = 0$ with $k \neq 0, n$, then the zero x_k must be of multiplicity $m > 1$, because otherwise in view of (1) we can find ξ arbitrarily close to x_k with $|f(\xi)| > 1$. If we split up these m zeroes into 1 zero for the inverval $[x_{k-1}, x_k]$ and $m-1$ zeroes for $[x_k, x_{k+1}]$, then in the end we see that each interval $[x_k, x_{k+1}]$ (now k runs from 0 to $n-1$) has at least one zero of P. By the splitting this gives a correct counting of the zeros. □

Let's now prove that $a_n \leq 2^{n-1}$. Suppose that $a_n > 2^{n-1}$. Define $P(x) = \frac{2^{n-1}}{a_n}f(x) - T_n(x)$. Then $\deg(P) \leq n-1$. Because of the lemma, we see that $P = 0$. Hence $f(x) = \frac{a_n}{2^{n-1}}T_n(x)$, which contradicts the conditions on f.
The only thing left to show is that $|f(\xi)| \leq 2^{n-1}|\xi|^n$ for all $\xi \in \mathbf{R}$ with $|\xi| > 1$. So suppose that there is a ξ violating this property. Then without loss of generality we may assume that $\xi > 1$, otherwise replace $f(x)$ by $(-1)^n f(-x)$. There are two cases to distinguish: $f(\xi) > 2^{n-1}\xi^n$ and $f(\xi) < -2^{n-1}\xi^n$.
In the case $f(\xi) > 2^{n-1}\xi^n$ look at the polynomial $P(x) = f(x) - T_n(x)$. First note that P is nonzero, otherwise $f(x) = T_n(x)$, which is a contradiction. The lemma implies that P has at least n zeroes on $[-1,1]$. It follows that $\deg(P) = n$ and $a_n < 2^{n-1}$. We can see that $f(\xi) > 2^{n-1}\xi^n \geq T_n(\xi)$ so $P(\xi) > 0$. The leading coefficient of P is negative so P must have a zero on (ξ, ∞). But then P has at least $n+1$ zeroes, which is again a contradiction.
In the case $f(\xi) < -2^{n-1}\xi^n$ the same argument applies with $P(x) = -f(x) - T_n(x)$.

Problem 2006/1-D Let G be a group such that the maps $f_m, f_n : G \to G$ given by $f_m(x) = x^m$ and $f_n(x) = x^n$ are both homomorphisms.

1. Show that G is Abelian if (m,n) is one of the pairs (4,11), (6,17).
2. Show that there are infinitely many pairs (m,n) such that G is Abelian.
3. Show that for every m there are infinitely many n such that G is Abelian.
4. Given a pair (m,n), how are we able to predict whether G is Abelian?

Solution This problem was solved by R. Bos, Peter Vandendriessche, B. Sury, and Jaap Spies. The solution below is based on that of R. Bos.
Let G be a group, and let $f_k : G \to G, x \mapsto x^k$ ($k \in \mathbf{Z}$).
Obviously, when G is Abelian, every f_k is a (homo)morphism. Conversely, we shall prove:

Theorem 1. *Suppose m and n satisfy the following: f_m and f_n are morphisms on a group G and $\gcd(m(m-1), n(n-1)) = 2$. Then G is Abelian. Moreover, for every m and n with $\gcd(m(m-1), n(n-1)) \neq 2$, there exists a non-Abelian group G such that f_m and f_n are morphisms on G.*
This completely classifies the pairs (m,n) mentioned in the problem. In particular, it provides an easy answer for all parts of the problem. For instance, given any m (different from 0,1) and any integer a we can take $n = am(m-1) - 1$ and easily check that the condition of the first part in the theorem is satisfied. Hence for every m there are infinitely

many n such that G is Abelian.

To prove the theorem, let us first introduce the following notation. $G^n = \Im(f_n)$ is the image of G under f_n , $C(G)$ is the center of G (the set of group elements h for which $gh = hg$, for all $g \in G$), $M = M(G) = \{n \in \mathbf{Z} | f_n$ is a morphism on $G\}$, and $A = A(G) = \{n \in \mathbf{Z} | f_n$ is a antimorphism on $G\}$ (that is, $f_n(xy) = f_n(y)f_n(x)$).

Lemma 1. *If G is a group and G^n, $C(G)$, M and A are as defined above, the following statements hold for all $n, k \in \mathbf{Z}$.*
i. $n \in M \Leftrightarrow -n \in A$,
ii. $n, kn \in M \Leftrightarrow n, n - kn \in M$,
iii. $n \in M \Leftrightarrow 1 - n \in M$,
iv. $n, -n \in M \Leftrightarrow n \in M \wedge G^n$ is abelian $\Longleftrightarrow n\mathbf{Z} \subset M$,
v. $n, -n \in M \Rightarrow G^n \subseteq C(G)$,
vi. If $k, n \in M$, then $k \times n \in M$.

Proof. (i) $(xy)^n = x^n y^n \Leftrightarrow (xy)^{-n} = y^{-n} x^{-n}$,
(ii) It suffices to prove '⇒'. To do so, first note that for every k we have $(uv)^k = u(vu)^{k-1} v$ (this also holds for negative k). Since $kn, n \in M$ we see that

$$x^{kn} y^{kn} = ((xy)^n)^k = (x^n y^n)^k = x^n (y^n x^n)^{k-1} y^n = x^n ((yx)^n)^{k-1} y^n,$$

hence $x^{kn-n} y^{kn-n} = (yx)^{kn-n}$, from which it follows that $kn - n \in A$, and $n - kn \in M$.
(iii) Apply (ii) to the pair $(1, n)$
(iv) Suppose n and $-n \in M$. According to (i), $n \in M \cap A$, hence $x^n y^n = (xy)^n = y^n x^n$, which implies that G^n is an abelian subgroup of G. As $n \in M$ and G^n is abelian, we see that $(xy)^{nt} = (x^n y^n)^t = x^{nt} y^{nt}$ since x^n and y^n commute. The last implication is trivial.
(v) We already know from (iv) that G^n is abelian, so $xy^n x^{-1} = (xyx^{-1})^n = x^n y^n x^{-n} = y^n$
(vi) Suppose $k, m \in M$, then $(xy)^{km} = (x^k y^k)^m = x^{km} y^{km}$. □

Corollary 1. *G is abelian $\Leftrightarrow -1 \in M \Leftrightarrow 2 \in M$.*

Proof. Since $1 \in M$, Lemma 1 *(iv)* and *(iii)* show that G is abelian iff $-1 \in M$, iff $2 \in M$.□

Lemma 2.
i. Suppose $m\mathbf{Z} \subseteq M$ and $n \in M$, then $n + m\mathbf{Z} \subseteq M$.
ii. Suppose $m\mathbf{Z}, n\mathbf{Z} \subseteq M$ and $k = \gcd(m, n)$, then $k\mathbf{Z} \subseteq M$.

Proof. (i) If $k = am + n$, then since am and n belong to M we have $(xy)^k = (xy)^{am}(xy)^n = x^{am} y^{am} x^n y^n$. Moreover $G^m \subseteq C(G)$ (Lemma 1 *(v)*), so y^{am} and x^n commute, hence $x^{am} y^{am} x^n y^n = x^{am} x^n y^{am} y^n = x^k y^k$.
(ii) From (i) we see that $m\mathbf{Z} + n\mathbf{Z} \subseteq M$. Since $k\mathbf{Z} = m\mathbf{Z} + n\mathbf{Z}$ we are done. □

Lemma 3. *Suppose $n \in M$. If $k = n(n-1)$, then $k, -k \in M$.*

Proof. Apply Lemma 1(iii) and (vi) a number of times: from $n \in M$ we see that $1 - n \in M$, so $-k = n(1-n) \in M$, but also $n^2 \in M$, therefore (Lemma 1 *(iii)*) $1 - n^2 \in M$. Since both $1 - n \in M$, and $1 - n^2 \in M$ and $1 - n | 1 - n^2$ Lemma 1 *(ii)* shows that $1 - n - (1 - n^2) = k \in M$. □

Corollary 2. *Suppose $n \in M$. Then $n(n-1)\mathbf{Z} \subseteq M$.*

Proof. Apply Lemma 3 and Lemma 1 *(iv)*. □

Proposition 1. *Suppose m and n both belong to M. Let $r = m(m-1)$ and $s = n(n-1)$. If $\gcd(r, s) = 2$, then G is abelian.*

Proof. Corollary 2 implies that $r\mathbf{Z}, s\mathbf{Z} \subseteq M$ and Lemma 2 *(ii)* shows that $2\mathbf{Z} \subseteq M$. Hence G is abelian by Corollary 1. □

Proposition 2. *Suppose r and s are as above. If* $\gcd(r,s) \neq 2$ *then there exists a non–abelian group G such that m and n both belong to M.*

Proof. Note that r and s have a common factor p^i where p is prime and $i > 0$ (and $i > 1$ if $p = 2$). Then p^i divides $r = m(m-1)$ hence p^i divides m or $m-1$. Suppose p^i divides m and similarly that p^i divides n. We shall define a finite non-abelian group $G = G(p)$ with p^3 elements in such a way that when p is odd we have $x^p = 1$ for every $x \in G$, and when $p = 2$, $x^4 = 1$ for every $x \in G$. This shows that in all cases $x^m = 1$ and $x^n = 1$ for every $x \in G$. In particular m and n belong to M. The same conclusions hold if for instance p^i divides $m-1$, since then $x^{m-1} = 1$, hence $x^m = x$, which again shows that $m \in M$. □

So let's proceed to the construction of the group $G = G(p)$. This will be a subgroup of the general linear group $GL_3(\mathbf{F}_p)$ of degree 3 over the finite field with p elements consisting of the matrices

$$\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

but more easily represented as the set of all elements $(x,y,z) \in \mathbf{F}_p^3$ with $(x,y,z) \times (x',y',z') = (x+x', y+y', z+z'+xy')$. It is easily verified that this defines a non–abelian group with unit $(0,0,0)$ and $(x,y,z)^n = (nx, ny, nz + \frac{1}{2}n(n-1)xy)$. In particular $(x,y,z)^p = (0,0,0)$ for odd p and $(x,y,z)^4 = (0,0,0)$ for the case $p = 2$ as was required.

Problem 2006/2-* Even though the problem was place in NAW 2006/2, we have already received several solutions and have decided to close the problem for submissions.

Prove or disprove that if $\binom{2n+1}{n} \equiv 1 \bmod n^2+n+1$ where n^2+n+1 is a prime, then $n = 8$.

Solution This problem was solved by Thomas Decru, Ruud Jeurissen, and Gerd Verbouwe. All of them had the following solution.
Choosing $n = 24$, we find that n^2+n+1 is a prime and $\binom{2n+1}{n} \equiv 1 \bmod n^2+n+1$. Thus the statement is refuted. Gerd Verbouwe showed that this is the only example for $n < 309$ other than $n = 8$.

Remark Hennie ter Morsche noticed that the solution of problem 2005/3-A is more general. Since $f(x)+1 = f(x-1)$ we find that f is the sum of $-x$ and the solutions of $g(x) = g(x-1)$. But for g we can choose an arbitrary continuous function with period 1.