Solutions for the AAC Competition Problems 2011

1. We will say that an element of a group is *stable* if it is fixed by every automorphism of the group. Describe all finite groups with the property that at least half of the elements are stable.

Solution: First we observe that all stable elements are central because they are not moved by inner automorphisms. Hence the index of the centre is at most 2. But recall that the quotient by the centre cannot be cyclic, so in fact the centre is the entire group, that is, the group is abelian.

Let us denote our abelian group by G and use additive notation. Being an automorphism of G, the map $x \mapsto -x$ does not move stable elements. Hence nontrivial stable elements have order 2, and G has a subgroup isomorphic to $\mathbb{Z}_2 \oplus \cdots \oplus \mathbb{Z}_2$ of index at most 2. Recalling the fundamental theorem on abelian groups, we see that G itself is isomorphic to either $\mathbb{Z}_2^n$ or $\mathbb{Z}_4 \oplus \mathbb{Z}_2^n$ where n is a nonnegative integer.

Suppose $G = \mathbb{Z}_2^n$. If $n \geq 2$ then G has no nontrivial stable elements. Indeed, for any $i \geq 2$, the map $(x_1, x_2, \ldots, x_n) \mapsto (x_1 + x_i, x_2, \ldots, x_n)$ is an automorphism of G, and it moves elements with nonzero i-th component. Hence, any stable element must have the form $(a, 0, \ldots, 0)$, but this is moved by the automorphism $(x_1, x_2, x_3, \ldots, x_n) \mapsto (x_1, x_1 + x_2, x_3, \ldots, x_n)$ unless $a = 0$.

Now suppose $G = \mathbb{Z}_4 \oplus \mathbb{Z}_2^n$. Then G has only one nontrivial stable element, namely, $(2, 0, \ldots, 0)$. Indeed, for any $i \geq 1$, the map $(x_0, x_1, \ldots, x_n) \mapsto (x_0 + 2x_i, x_1, \ldots, x_n)$ is a well-defined automorphism of G, and it moves elements with nonzero i-th component. Hence, any stable element must have the form $(a, 0, \ldots, 0)$, but this is moved by the automorphism $x \mapsto -x$ unless $a = 0$ or $a = 2$.

Answer: the cyclic groups of orders 1, 2 and 4.

2. The *centralizer* of a permutation is the set of all permutations that commute with it. What is the minimum number of elements in the centralizer of a permutation in S_n?

Solution: If $n \leq 2$ then S_n is abelian and the centralizer is the entire group. From now on, assume $n \geq 3$. Consider first the cycle $\sigma = (1, 2, \ldots, n-1)$. We claim that the centralizer of σ consists only of the powers of σ. Indeed, if τ is a permutation commuting with σ then $\sigma(\tau(n)) = \tau(\sigma(n)) = \tau(n)$, so $\tau(n)$ is a fixed point of σ, that is, $\tau(n) = n$. Denote $\tau(1) = s$. Then $s < n$ and $\tau(2) = \tau(\sigma(1)) = \sigma(\tau(1)) = \sigma(s) = s + 1$, etc. Hence $\tau = \sigma^s$, as claimed. We have proved that there exists a permutation whose centralizer has order $n - 1$.

Any $\sigma \in S_n$ can be uniquely written as a product of disjoint cycles: $\sigma = \sigma_1 \cdots \sigma_k$ where $k \geq 0$ and each σ_i has length $\ell_i \geq 2$. Note that the number of fixed points of σ is equal to $m = n - \sum \ell_i$. Since disjoint cycles commute with each other, σ commutes with all permutations of the form $\tau = \sigma_0 \sigma_1^{s_1} \cdots \sigma_k^{s_k}$

where σ_0 is any permutation of the fixed points of σ. Note that σ_0 and the congruence classes of s_i mod ℓ_i are uniquely determined by τ. We have $m!$ choices for σ_0 and ℓ_i choices for each s_i, hence the centralizer of σ contains at least $m! \prod \ell_i$ permutations. Let us show that this number is greater than or equal to $n-1$.

Indeed, for any $x, y \geq 2$ we have $xy \geq x+y$ since $(x-1)(y-1) \geq 1$. Hence, if $m \geq 2$ then

$$m! \prod \ell_i \geq m \prod \ell_i \geq m + \sum \ell_i = n.$$

If $m \leq 1$ then we obtain:

$$m! \prod \ell_i = \prod \ell_i \geq \sum \ell_i = n - m \geq n - 1,$$

as required.

Answer: n if $n \leq 2$ and $n-1$ if $n \geq 3$.

3. Prove that the binomial coefficients $\binom{2}{2}, \binom{3}{2}, \binom{4}{2}, \binom{5}{2}, \binom{6}{2}, \ldots$ give all possible remainders modulo n if and only if n is a power of 2.

Solution: First suppose n is not a power of 2. Then there exists a prime $p > 2$ that divides n. If the function $\binom{x}{2} = \frac{x(x-1)}{2}$ gives all possible remainders mod n, as x ranges over the integers $2, 3, \ldots$, then it also gives all possible remainders mod p. Since 2 is invertible mod p, we conclude that $f(x) = x(x-1)$ also gives all possible remainders mod p. Since the value $f(x)$ mod p depends only on the congruence class of x mod p, we can regard f as a function $\mathbb{Z}_p \to \mathbb{Z}_p$. This function takes value 0 for $x = 0$ and $x = 1$, so it cannot be surjective — a contradiction.

Now let $n = 2^m$. Note that $\frac{x(x-1)}{2}$ is defined for all integers x and the remainder of $\frac{x(x-1)}{2}$ mod n is repeated with period $2n$. We will prove that $\frac{x(x-1)}{2}$ gives all possible remainders mod n as x ranges over the set $\{1, \ldots, n\}$.

It is sufficient to verify that the values $\frac{x(x-1)}{2}$ and $\frac{y(y-1)}{2}$, where $x, y \in \{1, \ldots, n\}$, cannot coincide mod n unless $x = y$. Since the difference $\frac{x(x-1)}{2} - \frac{y(y-1)}{2}$ vanishes for $x = y$, it should be a multiple of $(x-y)$ in the ring $\mathbb{Q}[x, y]$. Indeed, it is easy to find an explicit factorization:

$$\frac{x(x-1)}{2} - \frac{y(y-1)}{2} = \frac{(x-y)(x+y-1)}{2}.$$

The right-hand side is not divisible by n if $x, y \in \{1, \ldots, n\}$ and $x \neq y$, because only one of the numbers $x-y$ and $x+y-1$ is even and, after division by 2, it gives a nonzero integer less than n.

There is an alternative argument, which generalizes to $\binom{x}{k}$ for any $k \geq 2$. In order to show that the congruence $\frac{x(x-1)}{2} \equiv a \pmod{2^m}$ has a solution for any a, we first rewrite it as $x(x-1) \equiv 2a \pmod{2^{m+1}}$ and then apply Hensel's Lemma to the polynomial $f(x) = x(x-1) - 2a \in \mathbb{Z}[x]$. For $m = 0$, the congruence

reads $x(x-1) \equiv 0 \pmod 2$, which has two simple roots: $\xi_0 \equiv 0$ and $\eta_0 \equiv 1$. By Hensel's Lemma, ξ_0 lifts to a (unique) root mod 2^{m+1}, that is, there exists an integer ξ_m such that $\xi_m \equiv \xi_0 \pmod 2$ and $f(\xi_m) \equiv 0 \pmod{2^{m+1}}$. (Of course, the same can be said about η_0.)

Remark: In addition to the periodicity mentioned above, the function $\binom{x}{2} = \frac{x(x-1)}{2} \bmod n$ has the following mirror symmetry: its value does not change if we replace x by $2n+1-x$.

4. Consider the additive group of polynomials in one variable with rational coefficients of degree at most 5 that take integer values at all integers. This group contains a remarkable subgroup that consists of the polynomials with integer coefficients. Find the index of this subgroup.

Solution: Suppose that a polynomial $f \in \mathbb{Q}[x]$ has degree n and takes integer values at all integers. We claim that the denominators of the coefficients of f (written in lowest terms) are divisors of $n!$. Indeed, we can recover f from its values $f(0), f(1), \ldots, f(n)$ using Lagrange Interpolation Formula:

$$f(x) = \sum_{i=0}^{n} f(i) \prod_{j \neq i} \frac{(x-j)}{(i-j)}.$$

Up to the sign, the denominator of the i-th term in the sum above has the form $i!(n-i)!$, which is a divisor of $n!$. On the other hand, the polynomials

$$p_0(x) = 1,\ p_1(x) = x,\ p_2(x) = \frac{x(x-1)}{2!},\ p_3(x) = \frac{x(x-1)(x-2)}{3!}, \ldots$$

take integer values at all integers (proof by induction on k and x using the relations $p_k(0) = 0$ and $p_k(x+1) - p_k(x) = p_{k-1}(x)$ for $k \geq 1$). Note that the highest term of $p_k(x)$ is $\frac{1}{k!}x^k$. It follows by induction on $n = \deg f$ that f can be uniquely written as a linear combination with integer coefficients of the polynomials $p_0, p_1, \ldots, p_n$. In other words, the set $\{p_0, p_1, \ldots, p_n\}$ is a basis for the additive group of polynomials in $\mathbb{Q}[x]$ of degree at most n that take integer values at all integers.

Now if $f \in \mathbb{Z}[x]$ has degree n then f can be uniquely written as a linear combination with integer coefficients of the monic polynomials $p_0,\ 1!p_1, \ldots,\ n!p_n$ (again by induction on n). Hence, the set $\{p_0,\ 1!p_1, \ldots,\ n!p_n\}$ is a basis for the subgroup consisting of the polynomials in $\mathbb{Z}[x]$ of degree at most n. It follows that the quotient group is isomorphic to $\mathbb{Z}_{2!} \oplus \mathbb{Z}_{3!} \oplus \cdots \oplus \mathbb{Z}_{n!}$.

Answer: the index is $2! \cdot 3! \cdot 4! \cdot 5! = 34560$.

5. We are given a table of size 3000×3000 filled with elements of the field $\mathbb{Z}_3$. It is known that the difference of any two columns contains exactly 1000 of 0's, of 1's and of 2's. Prove that the difference of any two rows has the same property.

Solution: We are given a square matrix $A = (a_{jk})$ of size $n = 3000$ where $a_{jk} \in \mathbb{Z}_3$. Let ε be a primitive complex cube root of unity, say, $\varepsilon = \exp\frac{2\pi i}{3}$. Then, for $a \in \mathbb{Z}_3$, we have a well-defined complex number ε^a. Consider the complex matrix $B = (b_{jk})$ where $b_{jk} = \varepsilon^{a_{jk}}$. Since $1+\varepsilon+\varepsilon^2 = 0$, the condition on the columns of A implies that any two columns of B are orthogonal with respect to the Hermitian inner product on $\mathbb{C}^n$ defined by $(x, y) = \sum_{j=1}^n x_i\bar{y}_j$, where bar denotes complex conjugate. Hence the matrix $U = \frac{1}{\sqrt{n}}B$ is unitary: $U^*U = I$ and, consequently, $UU^* = I$, where $*$ denotes the Hermitian adjoint (that is, conjugate transpose). Therefore, the rows of B are also pairwise orthogonal with respect to the Hermitian inner product. But the inner product of any two rows of B has the form $n_0 + n_1\varepsilon + n_2\varepsilon^2$, which can be zero only if $n_0 = n_1 = n_2$ (prove it!). The result follows.

6. Wedderburn Theorem states that all finite division rings are commutative. We will say that a unital associative ring is an *anti-division ring* if it does not contain invertible elements other than 1. Prove the following "Anti-Wedderburn Theorem": all finite anti-division rings are commutative.

Solution: Let R be an anti-division ring. First of all, since -1 is always invertible, we have $-1 = 1$, so R is an algebra over the field $\mathbb{Z}_2$. Suppose R is finite. Then, as a vector space over $\mathbb{Z}_2$, it has a finite dimension, say, n. We will prove that every element $a \in R$ is an idempotent, that is, $a^2 = a$.

Fix $a \in R$. Since the powers $1, a, \ldots, a^n$ are linearly dependent over $\mathbb{Z}_2$, we see that a is annihilated by some monic polynomial $f \in \mathbb{Z}_2[x]$ of degree at most n. Choose f of minimal possible degree. Then any polynomial $g \in \mathbb{Z}_2[x]$ with the property $g(a) = 0$ will have to be a multiple of f. It follows that f is uniquely determined by a. It is called *the minimal polynomial* of a. (This concept should be familiar in the context of matrices.)

If $a \neq 1$ then the constant term of f must be zero. Indeed, otherwise we would have $f(x) = 1+xg(x)$ for some $g \in \mathbb{Z}_2[x]$ and hence $0 = f(a) = 1+ag(a) = 1 + g(a)a$, which would imply the invertibility of a, contradicting the definition of anti-division ring. Therefore, we can write $f(x) = xg(x)$. Moreover, g cannot have zero constant term, for otherwise we would have $g(a)^2 = 0$ [because $g(x)^2$ is divisible by $xg(x) = f(x)$] and $g(a) \neq 0$ [because f is minimal], hence the element $b = 1+g(a)$ would be invertible (with $b^{-1} = b$) and distinct from 1. We have proved that if $a \neq 1$ then f is divisible by x but not by x^2. By a similar argument, if $a \neq 0$ then f is divisible by $x + 1$ but not by $(x + 1)^2$.

Now we are ready to prove that $a^2 = a$ for all $a \in R$. If $a = 0$ or 1, this is clear. Assume $a \neq 0, 1$. Then the minimal polynomial f can be written as $f(x) = x(x + 1)g(x)$ where g is not divisible by either x or $x + 1$. Consider $h(x) = x(x + 1) + g(x)$. Clearly, this polynomial is not divisible by x, $x + 1$ or any factor of g. Therefore, f and h are coprime. It follows that there exist $u, v \in \mathbb{Z}_2[x]$ such that $uf + vh = 1$, hence $v(a)h(a) = 1 = h(a)v(a)$. By definition of anti-division ring, we must have $h(a) = 1$. But this means that the polynomial $h(x) + 1 = x(x + 1) + g(x) + 1$ annihilates a, so its degree is

greater than or equal to $\deg f = 2 + \deg g$ (by minimality of f). This is possible only if $g = 1$, that is, $f(x) = x(x+1)$, which implies $a^2 = a$.

Finally, for all $a, b \in R$, we have $a^2 = a$, $b^2 = b$ and $(a+b)^2 = a+b$. But $(a+b)^2 = a^2 + ab + ba + b^2 = a + b + ab + ba$, so $ab + ba = 0$, that is, $ab = ba$.

Remark: Here is a more conceptual proof of the fact that $a^2 = a$ for any $a \in R$. Let $f \in \mathbb{Z}_2[x]$ be the minimal polynomial of a. Then the subalgebra A of R generated by a is isomorphic to the quotient $\mathbb{Z}_2[x]/(f)$. Write f as a product of powers of irreducible polynomials in $\mathbb{Z}_2[x]$: $f = g_1^{s_1} \cdots g_k^{s_k}$. Then, by Chinese Remainder Theorem, the ring A is isomorphic to the direct product $\mathbb{Z}_2[x]/(g_1^{s_1}) \times \cdots \times \mathbb{Z}_2[x]/(g_k^{s_k})$. Note that all factors must be anti-division rings, too. So, suppose that $B = \mathbb{Z}_2[x]/(g^s)$ is an anti-division ring where $g \in \mathbb{Z}_2[x]$ is irreducible and s is a positive integer. For $h \in \mathbb{Z}_2[x]$, we will write $\bar{h} = h + (g^s)$. If $s > 1$ then $\bar{g} \neq 0$ is a nilpotent element of B and hence $1 + \bar{g}$ is invertible and distinct from 1. Therefore, $s = 1$. But then $B = \mathbb{Z}_2[x]/(g)$ is a field, so it has invertible elements other than 1 unless it is isomorphic to $\mathbb{Z}_2$. We have proved that A is the direct product of copies of $\mathbb{Z}_2$. Then, clearly, every element of A is an idempotent.