

## Problem 2

France 2

We solved completely questions 1), 2) and 3). Essentially, the study of  $\frac{k(k+1)}{2}$  is the same as the study of  $k^2$  modulo  $p^n$ , for  $p$  odd.

For  $p$  even it's a bit more complicated because of the 2 at the denominator.

Finally, to find  $u_n$  for every  $n$ , we prove a property of multiplicativity of  $(u_n)$ , which is in fact true for every polynomial (and not only  $\frac{k(k+1)}{2}$ ).

## 0.1 Question 1

Consider the map  $f : \{0, 1, \dots, 2^\alpha - 1\} \rightarrow \mathbf{Z}/2^\alpha\mathbf{Z}$  defined by  $f(n) = \frac{n(n+1)}{2} \pmod{2^\alpha}$ . We claim that  $f$  is bijective. For cardinality reasons, it is enough to prove that  $f$  is injective. If  $a, b \in \{0, 1, \dots, 2^\alpha - 1\}$ , then

$$f(a) = f(b) \Leftrightarrow \frac{a(a+1)}{2} \equiv \frac{b(b+1)}{2} \pmod{2^\alpha} \Leftrightarrow (a-b)(a+b+1) \equiv 0 \pmod{2^{\alpha+1}}.$$

On the other hand,  $a-b$  and  $a+b+1$  have different parities, so the congruence  $(a-b)(a+b+1) \equiv 0 \pmod{2^{\alpha+1}}$  is equivalent to  $a \equiv b \pmod{2^{\alpha+1}}$  or  $a+b+1 \equiv 0 \pmod{2^{\alpha+1}}$ . The first congruence yields  $a = b$ , since  $a, b \in \{0, 1, \dots, 2^\alpha - 1\}$ . The second congruence is impossible, as  $0 < a+b+1 < 2^{\alpha+1}$ .

This shows that  $u_n = n$  when  $n$  is a power of 2.

## 0.2 Question 2

Let  $p$  be an odd prime. Note that

$$T_k = \frac{k(k+1)}{2} = \frac{(2k+1)^2 - 1}{8}.$$

Since  $p$  is odd, 8 is invertible mod  $p^\alpha$  and  $x \rightarrow 2x+1$ , respectively  $x \rightarrow \frac{x-1}{8}$  are permutations of  $\mathbf{Z}/p^\alpha\mathbf{Z}$  for  $\alpha \geq 1$ . So finding  $u_{p^\alpha}$  comes down to finding the number of squares in  $\mathbf{Z}/p^\alpha\mathbf{Z}$ .

For an integer  $n$ , let  $\bar{n}$  be the residue class of  $n$  modulo  $p^\alpha$ . Suppose that  $\bar{n}$  is a nonzero residue class, which is a square in  $\mathbf{Z}/p^\alpha\mathbf{Z}$ . Hence, there exists  $m \in \mathbf{Z}$  such that  $n \equiv m^2 \pmod{p^\alpha}$ . Let  $p^j$  be the largest power of  $p$  dividing  $m$ . Then  $p^{2j}$  is the largest power of  $p$  dividing  $m^2$ . Since  $\bar{n} \neq 0$ , we obtain  $2j < \alpha$ . By definition, there exists  $k$  relatively prime to  $p$  such that  $m = p^j k$ . We deduce that  $\bar{n} = \overline{p^{2j} k^2}$ .

Let us consider now  $j, j_1$  and  $k, k_1$  such that  $\max(2j, 2j_1) < \alpha$  and  $\overline{p^{2j} k^2} \equiv \overline{p^{2j_1} k_1^2} \pmod{p^\alpha}$ . If  $j < j_1$ , we obtain  $k^2 \equiv p^{2(j_1-j)} k_1^2 \pmod{p^{\alpha-2j}}$ , which is impossible, as  $p$  does not divide  $k$ . So  $j \geq j_1$  and, by symmetry, we conclude that  $j = j_1$  and  $k^2 \equiv k_1^2 \pmod{p^{\alpha-2j}}$ . This last congruence is equivalent to  $k \equiv \pm k_1 \pmod{p^{\alpha-2j}}$  (we are using here that  $p > 2$ , so  $p$  cannot divide simultaneously  $k+k_1$  and  $k-k_1$ ).

The previous two paragraphs show that the nonzero squares of  $\mathbf{Z}/p^\alpha\mathbf{Z}$  are precisely the residue classes  $\overline{p^{2j} k^2}$ , where  $2j < \alpha$  and  $k \in \{1, \dots, \frac{p^{\alpha-2j}-1}{2}\}$  is prime to  $p$ . Moreover, all these classes are distinct. Hence, the total number of squares is

$$1 + \sum_{2j < \alpha} \frac{p^{\alpha-2j} - p^{\alpha-2j-1}}{2}.$$

Let  $N = \left\lfloor \frac{\alpha-1}{2} \right\rfloor$ . Then

$$1 + \sum_{2j < \alpha} \frac{p^{\alpha-2j} - p^{\alpha-2j-1}}{2} = 1 + \frac{p^{\alpha-1}(p-1)}{2} \sum_{j=0}^N p^{-2j} =$$

$$= 1 + \frac{p^{\alpha-1}(p-1)}{2} \frac{1-p^{-2(N+1)}}{1-p^{-2}} = 1 + \frac{p^{\alpha+1}}{2(p+1)}(1-p^{-2(N+1)}).$$

Explicitly, if  $\alpha$  is even, then

$$u_{p^\alpha} = \frac{p^{\alpha+1} + p + 2}{2(p+1)},$$

while if  $\alpha$  is odd, we obtain

$$u_{p^\alpha} = \frac{p^{\alpha+1} + 2p + 1}{2(p+1)}.$$

### 0.3 Question 3

We will prove that if  $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$  is the prime factorization of  $n$  (with  $p_i$  distinct prime numbers and  $\alpha_i$  positive integers), then

$$u_n = \prod_{i=1}^k u_{p_i^{\alpha_i}}.$$

Let

$$X_n = \{T_l \pmod{n} \mid 0 \leq l < n\}.$$

We will construct a bijection between  $X_n$  and  $\prod_{i=1}^k X_{p_i^{\alpha_i}}$ , which will be enough to prove our previous claim.

Let  $x \in X_n$ , say  $x = T_l \pmod{n}$  for some  $0 \leq l < n$ . Associate to  $x$  the  $k$ -tuple  $(T_l \pmod{p_1^{\alpha_1}}, \dots, T_l \pmod{p_k^{\alpha_k}})$ . Note that this  $k$ -tuple does not depend on the choice of  $l$  and belongs to  $\prod_{i=1}^k X_{p_i^{\alpha_i}}$ . We will check that this is a bijection.

First, assume that  $x = T_l \pmod{n}$  and  $y = T_s \pmod{n}$  have the same associated  $k$ -tuple. Then  $T_l \equiv T_s \pmod{p_i^{\alpha_i}}$  for all  $1 \leq i \leq k$ , so that  $T_l \equiv T_s \pmod{n}$  and  $x = y$ . Thus the previous map is injective.

Next, we will check that the map is onto. Pick a  $k$ -tuple  $(x_1, \dots, x_k) \in \prod_{i=1}^k X_{p_i^{\alpha_i}}$ . By definition, we can find  $0 \leq l_i < p_i^{\alpha_i}$  such that  $x_i = T_{l_i} \pmod{p_i^{\alpha_i}}$ . By the Chinese Remainder Theorem, there exists  $l \in \{0, 1, \dots, n-1\}$  such that  $l \equiv l_i \pmod{p_i^{\alpha_i+1}}$  for all  $1 \leq i \leq k$ . We claim that  $x := T_l \pmod{n}$  is sent to  $(x_1, \dots, x_k)$ . It is enough to prove that  $T_l \equiv T_{l_i} \pmod{p_i^{\alpha_i}}$  for all  $i$ . This follows from our choice of  $l$  and the fact that

$$T_l - T_{l_i} = \frac{(l - l_i)(l + l_i + 1)}{2}.$$