Let p be a prime and consider the function $f : \mathbb{F}_p \times \mathbb{F}_p \longrightarrow 0, 1$, defined by

$$f(x,y) = \begin{cases} 1 & \text{if } x < y \\ 0 & \text{else} \end{cases}$$

Where the inequality $<$ is defined by identifying $\mathbb{F}_p$ with $\{0, \dots, p-1\}$.

Proposition 1. *The function f is a polynomial in the variables x and y of degree p. Moreover, we have*

$$f(x,y) = \sum_{m=1}^{p-1} x^m y^{p-m} \frac{1}{m} + \text{ lower order terms.}$$

Proof. An explicit polynomial expression is given by

$$f(x,y) = \sum_{0 \le i < j < p} (1 - (x-i)^{p-1})(1 - (y-j)^{p-1}).$$

Each term in this sum gives 1 for $(x, y) = (i, j)$ and zero for all other tuples $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$. From this expression it is not at all clear that the degree of this polynomial is p, so we will rewrite it first, and then apply lemma 4 below. We will use the following identity:

$$(x-a)^{p-1} = \sum_{n=0}^{p-1} x^n a^{p-1-n},$$

which can be proved by multiplying both sides with $(x + a)$. Applying this we obtain the following expression for f:

$$f(x,y) = \sum_{0 \le i < j < p} \big(1 - \sum_{m=0}^{p-1} x^m i^{p-1-m}\big)\big(1 - \sum_{n=0}^{p-1} y^n j^{p-1-n}\big).$$

We now work this out distributively to get

$$\begin{aligned} f(x,y) = &\sum_{0 \le i < j < p} 1 \\ &- \sum_{0 \le i < j < p} \sum_{m=0}^{p-1} x^m i^{p-1-m} \\ &- \sum_{0 \le i < j < p} \sum_{n=0}^{p-1} y^n j^{p-1-n} \\ &+ \sum_{0 \le i < j < p} \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} x^m i^{p-1-m} y^n j^{p-1-n}. \end{aligned} \tag{1}$$

Since we are not interested in terms of degree strictly smaller than p, we only need to look at line (1). This line can be rewritten as

$$\sum_{m=0}^{p-1}\sum_{n=0}^{p-1} x^m y^n \sum_{0\le i<j<p} i^{p-1-m} j^{p-1-n}.$$

Now we can apply lemma 4 with $k = p-1-m$ and $l = p-1-n$. When $m+n > p$, then $k+l < p-2$ and the lemma tells us that the inner sum is zero, hence the polynomial is of degree at most p. When $m+n = p$, then $k+l = p-2$ and the lemma yields the value $-1/(k+1) = -1/(p-m)$ for the inner sum, which in $\mathbb{F}_p$ is the same as $1/m$ and so the result follows. $\square$

The following lemmas are each used in the proof of the next one, and lemma 4 was used to prove proposition 1.

Lemma 2. *Let p be a prime and P a polynomial over $\mathbb{F}_p$ of degree at most $p-2$, then*

$$\sum_{i=0}^{p-1} P(i) = 0 \text{ in } \mathbb{F}_p$$

Proof. Let d be the degree of P. We prove it by induction on d. For $d = 0$ P is constant and we get $pP(0) = 0$ in $\mathbb{F}_p$. Now suppose $d > 0$. Let P_1 be the polynomial of degree d defined by

$$P_1(x) = \binom{x+d}{d} = \frac{(x+1)\cdot\ldots\cdot(x+d)}{d!}.$$

This expression does not involve division by p as $d < p$, so we can view P_1 as a polynomial over $\mathbb{F}_p$. Write $P = aP_1 + P_2$, where P_2 has degree at most $d-1$. We have

$$\sum_{i=0}^{p-1} P(i) = a\sum_{i=0}^{p-1} P_1(i) + \sum_{i=0}^{p-1} P_2(i).$$

The last term is zero by induction hypothesis, so we have

$$\begin{aligned}\sum_{i=0}^{p-1} P(i) &= a\sum_{i=0}^{p-1} P_1(i)\\ &= a\sum_{i=0}^{p-1}\binom{i+d}{d}\\ &\overset{(2)}{=} a\binom{p+d}{d+1}\\ &= 0\end{aligned}$$

as $d+1$ is smaller than p. (We have $(p+d)!/((d+1)!(p-1)!)$, which is divisible by p.) $\square$

Here we have used the formula

$$\sum_{i=0}^{n} \binom{i+d}{d} = \binom{n+d+1}{d+1}, \tag{2}$$

which one can prove by induction on n.

Lemma 3. *Let p be an odd prime and let P and Q be polynomials over $\mathbb{F}_p$ of degree k and l respectively.*

(*a*) *if $k+l < p-2$, then*

$$\sum_{0 \le i < j < p} P(i)Q(j) = 0 \text{ in } \mathbb{F}_p.$$

(*b*) *if $k+l = p-2$ then*

$$\sum_{0 \le i < j < p} P(i)Q(j) = -b_P b_Q/(k+1),$$

where b_P (resp. b_Q) is the leading term of P (resp. Q).

Proof. We first prove (a) by induction on k. If $k=0$ then P is constant and our expression becomes

$$\sum_{j=0}^{p-1} jP(0)Q(j),$$

which is zero by the previous lemma as $xP(0)Q(x)$ is a polynomial of degree $l+1$, which is smaller than $p-1$. Now for the induction step assume $k>0$ and let P_1 be the polynomial of degree k defined by

$$P_1(x) = \binom{x+k}{k} = \frac{(x+1)\cdot \ldots \cdot (x+k)}{k!}.$$

We are not dividing by p as $k < p$, so we can consider this a polynomial over $\mathbb{F}_p$. Now write $P = aP_1 + P_2$, where P_2 is some polynomial of degree smaller than k. We have

$$\sum_{0 \le i < j < p} P(i)Q(j) = a \sum_{0 \le i < j < p} P_1(i)Q(j) + \sum_{0 \le i < j < p} P_2(i)Q(j).$$

This last term is zero by induction hypothesis. We have

$$\begin{aligned}
\sum_{0\le i<j<p} P(i)Q(j) &= a \sum_{0\le i<j<p} P_1(i)Q(j) \\
&= a\sum_{j=1}^{p-1} Q(j) \sum_{i=0}^{j-1} \binom{i+k}{k} \\
&\overset{(2)}{=} a\sum_{j=1}^{p-1} Q(j)\binom{j+k}{k+1} \\
&= a\sum_{j=0}^{p-1} Q(j)\binom{j+k}{k+1}
\end{aligned}$$

Since $Q(x)\binom{x+k}{k+1}$ is a polynomial of degree $k+l+1$, which is smaller than $p-1$, the previous lemma implies that the expression is zero.

We now prove (b). Everything is analogous until we arrive at the expression

$$a\sum_{j=0}^{p-1} Q(j)\binom{j+k}{k+1} = \sum_{j=0}^{p-1} R(j),$$

where $R(x) = aQ(x)\binom{x+k}{k+1}$ is now a polynomial of degree $p-1$. The leading term of this polynomial is $a \cdot b_Q/(k+1)!$, where b_Q is the leading term of Q. Note that since $P = aP_1 + P_2$, a is the leading term of P divided by the leading term of P_1. The leading term of P_1 is $1/(k!)$ and so

$$a = b_P k!$$

where b_P is the leading term of P. Therefore the leading term of R is $b_P b_Q k!/(k+1)! = b_P b_Q/(k+1)$. We now get

$$\begin{aligned}
\sum_{0\le i<j<p} P(i)Q(j) &= \sum_{j=0}^{p-1} R(j) \\
&= \sum_{j=0}^{p-1} b_P b_Q/(k+1) j^{p-1} + \text{ lower order terms}
\end{aligned}$$

By the previous lemma the lower order terms contribute nothing, so we get

$$\begin{aligned}
\sum_{0\le i<j<p} P(i)Q(j) &= \sum_{j=0}^{p-1} b_P b_Q/(k+1) j^{p-1} \\
&= \sum_{j=1}^{p-1} b_P b_Q/(k+1) \\
&= -b_P b_Q/(k+1).
\end{aligned}$$

Obviously we used that $j^{p-1} = 1$ for nonzero j in $\mathbb{F}_p$. □

The next lemma is a reformulation of the previous one:

Lemma 4. *Let* $k, l \geq 0$ *with* $k + l < p - 2$*, then*

$$\sum_{0 \leq i < j < p} i^k j^l = 0.$$

If $k, l \geq 0$ *with* $k + l = p - 2$ *then*

$$\sum_{0 \leq i < j < p} i^k j^l = \frac{-1}{k+1}.$$

(equalities are in $\mathbb{F}_p$)

Proof. Apply the previous lemma with $P(x) = x^k$ and $Q(x) = x^l$. $\square$

note that we consider zero to the power zero to equal one.