Let $p$ = 11

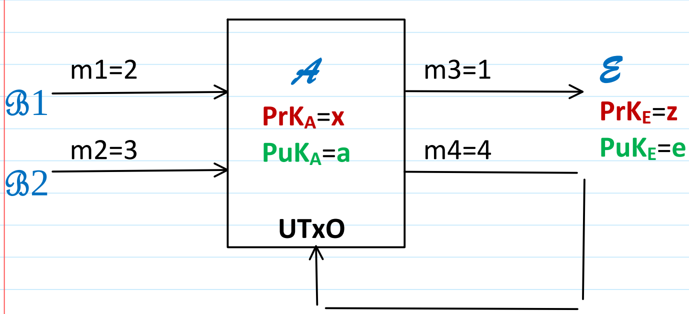
| $y$ mod 11 | | | $(-y)$ mod 11 | Explanation |
|---|---|---|---|---|
| 1 | odd | even | -1=10 | 1+(-1) = 1+10 = 11 = 0 mod 11 |
| 2 | even | odd | -2=9 | 2+(-2) = 2+9 = 11 = 0 mod 11 |
| 3 | odd | even | -3=8 | |
| 4 | even | odd | -4=7 | |
| 5 | odd | even | -5=6 | |
| 6 | even | odd | -6=5 | |
| 7 | odd | even | -7=4 | |
| 8 | even | odd | -8=3 | |
| 9 | odd | even | -9=2 | |
| 10 | even | odd | -10=1 | 10+(-10) = 10+1 = 11 = 0 mod 11 |

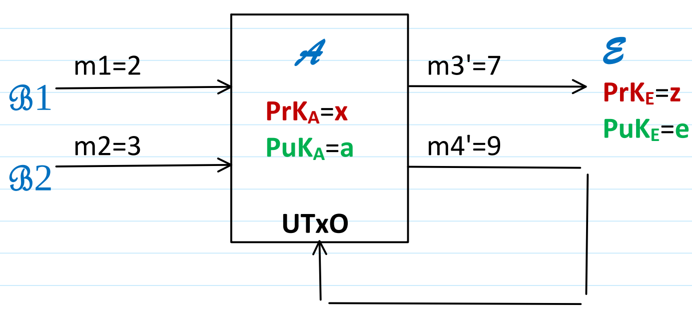
2+3 = 5 mod 11
7+9 = 16 = 5 mod 11

7 === -4 mod 11
9 === -2 mod 11

(-4)+(-2) = -6 mod 11 = 5 mod 11

Let Unspent Transactions Outputs - UTxO are made in bitcoins - BTC and as toy example take $p$ = 11




The balance equation is:
2+ 3 = 5 mod 11 = 1+4 = 5 mod 11

The balance equation is:
2+ 3 = 5 mod 11 = 7+9 = 16 mod 11 = 5

**4.3 Range proofs**.
How to prove that Alice spends the same sum $Ex = m_3 + m_4 = 5 = m_1 + m_2 = In$.

We will deal with **Elliptic Curves (EC), Elliptic Curve Groups (ECG)** and **Elliptic Curve Cryptosystem (ECCS)**

| **Elliptic Curve Group (ECG)** |
|---|
| Number of points **N** of Elliptic Curve with coordinates $(x, y)$ is an order of ECG. |
| Addition operation ⊞ of points in ECG: let points $P(x_P,y_P)$ and $Q(x_Q,y_Q)$ are in EC with coordinates $(x_P,y_P)$ and $(x_Q,y_Q)$ then $P$ ⊞ $Q = T$ with coordinates $(x_T,y_T)$ in EC. |
| Neutral element is group zero $O$ at the infinity (∞) of [XOY] plane. |
| Multiplication of any EC point $G$ by scalar $x$: $A=x*G$; $A=G$ ⊞ $G$ ⊞ $G$ ⊞ ...⊞ $G$; $x$–times. |
| Generator–Base Point $G$: ECG={ $i*G$; $i$=1,2,…,N}; $N*G=0$ and $q*G\neq 0$ if $q<N$. |

| **Elliptic Curve Cryptosystem (ECCS)** |
|---|

**PP**=(EC **secp256k1**; BasePoint-Generator $G$; prime $p$; param. $a$, $b$);
Parameters $a$, $b$ defines EC equation $y^2=x^3+ax+b$ **mod** $p$ over $F_p$.

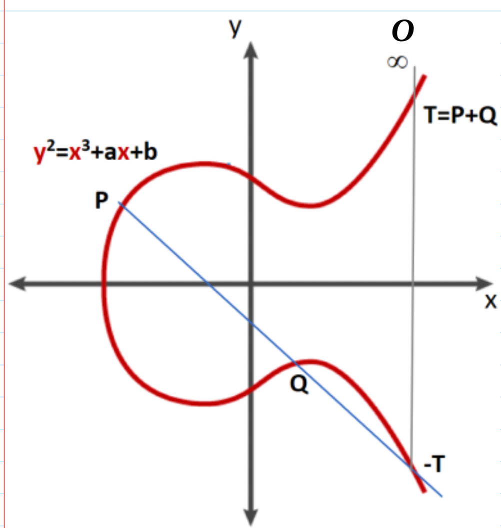
**PrK** $_{ECC}$=**x**;
>> **x**=randi($p$-1).

**PuK**$_{ECC}$ = $A$ = $G \boxplus G \boxplus G \boxplus \ldots \boxplus G$; $x$–times.

**Alice** $A$: **x**=.....; $A=(x_A, y_A)$;

Let $r$ <-- randi($p$) be a secret number.
Let $H = r * G$ be the other Generator in **EC**.
Both $G$ and $H$ are Public Parameters **PP** = ($G$, $H$) together with all others for Range Proofs.

We will use the following identities valid in EC algebra.
Let $u$, $v$ are integers < $p$.
Property 1: $(u + v)*P = u*P \boxplus v*P$ in literature it is replaced to --> $(u + v)P = uP + vP$
Property 2: $u*(P \boxplus Q) = u*P \boxplus u*Q$ in literature it is replaced to --> $u(P + Q) = uP + uQ$
Property 3: $u*T \boxminus u*T = u*(T \boxminus T) = u*O = O$;
$u*T \boxminus u*T = (u-u)*T = 0*T = O$.




For incomes $In = 5 = 101_b = (b_2\, b_1\, b_0)_b = b_2 \bullet 2^2 + b_1 \bullet 2^1 + b_0 \bullet 2^0 = 1\bullet 2^2 + 0\bullet 2^1 + 1\bullet 2^0 = 5$.

Generate random numbers $x_2$, $x_1$, $x_0$ in $Z_N$ (the set of positive integers do not exceeding the ***number N*** of points of Elliptic Curve) to be used as blinding factors.
Define also Pedersen Commitments $C_2$, $C_1$, $C_0$ for each $b_2$, $b_1$, $b_0$:

$$C_2 = x_2*G \boxplus (b_2\bullet 2^2)*H.$$
$$C_1 = x_1*G \boxplus (b_1\bullet 2^1)*H.$$
$$C_0 = x_0*G \boxplus (b_0\bullet 2^0)*H.$$

Then $x_2$, $x_1$, $x_0$ will always be a private keys $PrK_2$, $PrK_1$, $PrK_0$ to one part of the following
public keys $PuK_2$, $PuK_1$, $PuK_0$ respectively consisting of 2 components

$PrK_2 = x_2$; $PuK_2 = (PuK_{21}, PuK_{22}) = (C_2, C_2 \boxminus (b_2\bullet 2^2)*H)$.
$PrK_1 = x_1$; $PuK_1 = (PuK_{11}, PuK_{12}) = (C_1, C_1 \boxminus (b_1\bullet 2^1)*H)$.

$PrK_0 = x_0$; $PuK_0 = (PuK_{01}, PuK_{02}) = (C_0, C_0 \boxminus (b_0 \bullet 2^0) * H)$.

Clearly, in general for $i = 2, 1, 0$, if $b_i = 0$ --> $C_i = x_i * G \boxplus 0 * H = x_i * G$

if $b_i = 1$ --> $C_i = x_i * G \boxplus (1 \bullet 2^i) * H \boxminus (1 \bullet 2^i) * H = x_i * G$.

In our case when $(b_2 b_1 b_0)_b = (101)_b$ we have:

$b_2 = 1$ --> $PrK_2 = x_2$; $PuK_2 = (PuK_{22}) = (C_2 \boxminus (1 \bullet 2^2) * H) = x_2 * G \boxplus (1 \bullet 2^2) * H \boxminus (1 \bullet 2^2) * H = x_2 * G$.

$b_1 = 0$ --> $PrK_1 = x_1$; $PuK_1 = (PuK_{11}) = (C_1 \boxminus (0 \bullet 2^1) * H) = x_1 * G \boxplus (0 \bullet 2^1) * H = x_1 * G$.

$b_0 = 1$ --> $PrK_0 = x_0$; $PuK_0 = (PuK_{02}) = (C_2 \boxminus (1 \bullet 2^0) * H) = x_0 * G \boxplus (1 \bullet 2^0) * H \boxminus (1 \bullet 2^0) * H = x_0 * G$.

In our case for incomes $In = 5$ we have:

$$C = C_2 \boxplus C_1 \boxplus C_0 = x_2 * G \boxplus (b_2 \bullet 2^2) * H \boxplus x_1 * G \boxplus (b_1 \bullet 2^1) * H \boxplus x_0 * G \boxplus (b_0 \bullet 2^0) * H =$$

$$= (x_2 + x_1 + x_0) * G \boxplus ((1 \bullet 2^2) + (0 \bullet 2^1) + (1 \bullet 2^0)] * H =$$

$$= (x_2 + x_1 + x_0) * G \boxplus (1 \bullet 2^2 + 0 \bullet 2^1 + 1 \bullet 2^0) * H =$$

$$= (x_2 + x_1 + x_0) * G \boxplus 5 * H.$$

In other words, a blinding factor $x_i$ will always be the private key corresponding to one of $\{C_i, C_i - 2^i H\}$. Therefore we will be able to sign an amount $a$ in a transaction using the Borromean Ring Signature scheme of Section 3.4 with the ring:

$$\{\{C_0, C_0 - 2^0 H\}, ..., \{C_k, C_k - 2^k H\}\}$$

## 4.4 Range proofs in a blockchain

In the context of Monero we will use range proofs to commit to individual bit components and to prove that their sum equals the total amount committed. Therefore, it will not be necessary for the receiver nor any other party to know the blinding factors $x_i G$. In other words, it is sufficient to know that

$$\sum_{i=0}^{k} C_i = C$$

In the blockchain we will store only the commitments/keys $C_i$. The mining community will have to check that the equation above holds and that the private key of either $C_i$ or $C_i - 2^i H$ has been used to sign the amount.

The Borromean signature scheme requires knowledge of $x_i$ to produce a signature. In consequence, upon verifying this relationship between keys, any third party will be able to convince himself that amounts fall within ranges and that money is not being artificially *created*.

Till this place

In other words, a blinding factor xi will always be the private key corresponding to one of
fCi;Ci ⍰ 2iHg. Therefore we will be able to sign an amount a in a transaction using the
Borromean Ring Signature scheme of Section 3.4 with the ring:
ffC0;C0 ⍰ 20Hg; :::; fCk;Ck ⍰ 2kHgg
4.4 Range proofs in a blockchain

In the context of Monero we will use range proofs to commit to individual bit components and to prove that their sum equals the total amount committed. Therefore, it will not be necessary for the receiver nor any other party to know the blinding factors xiG. In other words, it is su cient to know that

Xk
i=0
Ci = C

In the blockchain we will store only the commitments/keys Ci. The mining community will have to check that the equation above holds and that the private key of either Ci or Ci ? 2iH has been used to sign the amount.

The Borromean signature scheme requires knowledge of xi to produce a signature. In consequence, upon verifying this relationship between keys, any third party will be able to convince himself that amounts fall within ranges and that money is not being arti cially created.