P 11.1

- **Public parameter creation:** A trusted party chooses an elliptic curve E over $\mathbb{F}_p$ and a point P of large prime order q in $E(\mathbb{F}_p)$.
- **Key creation:** Sarah chooses a secret signing key $1 \leqslant a \leqslant q-1$ and computes and publishes the verification key $A = aP$.
- **Signature:** Sarah chooses a document $D \in \mathbb{Z}/q\mathbb{Z}$ (e.g., a hashed message) and a random integer k mod q. She computes $kP \in E(\mathbb{F}_p)$ and then publishes the signature $D^{\text{sig}} = (S_1, S_2)$ given by:

$$S_1 \equiv x(kP) \bmod q, \qquad S_2 \equiv (D + aS_1)k^{-1} \bmod q.$$

- **Verification:** To verify the signature, Victor computes

$$V_1 = DS_2^{-1} \bmod q, \qquad V_2 = S_1 S_2^{-1} \bmod q$$

and checks that $x(V_1P + V_2A) \mod q = S_1$. (Here $x(Q)$ denotes the x-coordinate of a point $Q = (x(Q), y(Q))$ on E, and $x(Q) \bmod q$ means that we take the smallest positive representative of $x(Q) \in \mathbb{F}_p$ in $\{0, \ldots, p-1\} \subset \mathbb{Z}$ and then reduce it mod q).

Th: Verification step succeeds if Sarah signed the document

Let's compute the following:

$$V_1P + V_2A = DS_2^{-1}P + S_1S_2^{-1}A = S_2^{-1}(DP + S_1A) = S_2^{-1}(DP + S_1aP) = S_2^{-1}(D + S_1a)P$$

$$= k(D + aS_1)^{-1}(D + aS_1)P = kP \pmod q$$

So we have that

$$V_1P + V_2A = kP \pmod q$$

So we indeed have that

$$x(V_1P + V_2A) = S_1 \pmod q$$

because $S_1 = x(kP) \pmod q$ and we just saw that $V_1P + V_2A = kP \pmod q$. □

T 11.4

Theorem 11.4.1 Every integer $n \geq 0$ is the sum of 4 squares of integers:

$$\exists\, x_1, x_2, x_3, x_4 \in \mathbb{Z} \text{ s.t. } n = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Assume $n = p$ is an odd prime

a) **Th:** $\exists\, a, b \in \mathbb{Z}$ s.t. $a^2 + b^2 + 1 \equiv 0 \mod p$

We have that $\mathbb{F}_p$ is a finite field of p elements, with p odd prime.
In particular, $\mathbb{F}_p^\times$ has $p-1$ elements.

We define a square to be an element s s.t. there is an element v for which we can write $s = v^2$ in $\mathbb{F}_p$.

We want to reason about $\mathbb{F}_p^\times$, but first note that $0 \in \mathbb{F}_p$ is a square

Now we have $\mathbb{F}_p^\times = \{1, \dots, p-1\}$ being a set of even number of elements.
Moreover, $\mathbb{F}_p^\times$ is a cyclic group so we have
$\mathbb{F}_p^\times = \langle g \rangle = \{g^0, g, g^2, \dots, g^{p-2}\}$ for some g generator.

In general we must have that
- $g^0, g^2, g^4, \dots, g^{p-3}$ are surely squares
- $g^1, g^3, g^5, \dots, g^{p-2}$ are surely NOT squares

proof: **Th:** $g^1, g^3, g^5, \dots, g^{p-2}$ are surely NOT squares

The only way for $g^1, g^3, g^5, \dots, g^{p-2}$ to be squares is if the generator g is a square itself. But this cannot be because otherwise g could not be a generator, since it would be $g = h^2$ for some h and $\#\langle g \rangle = \frac{p-1}{2} < p-1$.

Therefore, if $g^1, g^3, g^5, \dots, g^{p-2}$ were to be squares, we would have a contradiction with the hypothesis.

So, out of the $p-1$ not-zero elements, $\frac{p-1}{2}$ are squares and $\frac{p-1}{2}$ are NOT squares.

In total, accounting also for the zero element $0 \in \mathbb{F}_p$, we will have $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ squares in $\mathbb{F}_p$.

From here, we want to prove that $\exists\, a, b \in \mathbb{F}_p$ s.t. $a^2 \equiv -(b^2+1) \mod p$.

Let us define the sets

$$S_1 := \{a^2 \bmod p : a \in \mathbb{F}_p\} \subseteq \mathbb{F}_p$$
$$S_2 := \{-b^2 - 1 \bmod p : b \in \mathbb{F}_p\} \subseteq \mathbb{F}_p$$

Note that $S_1 \cup S_2 = \mathbb{F}_p$.

Now let's reason about their cardinalities:

- Since there are $\frac{p+1}{2}$ squares in $\mathbb{F}_p$, it's clear that:
  $\#S_1 = \frac{p+1}{2}$.

- For the exact same reason, we also have that
  $\#S_2 = \frac{p+1}{2}$.
  This is due to the definition of S_2 and the fact that we are considering the squares b^2 for $b \in \mathbb{F}_p$, adding 1 to them and then taking the opposite.
  Thus, the number of such elements is the same as the number of squares in $\mathbb{F}_p$.

To conclude, we notice that we have $\#S_1 + \#S_2 = p+1$
This means that the two sets are not disjoint, but instead we have
$\exists z \in \mathbb{F}_p$ s.t. $S_1 \cap S_2 = \{z\}$.

Such element will be s.t. $z = a^2 \bmod p$ & $z = -(1+b^2) \bmod p$ for some $a, b \in \mathbb{F}_p$.

$\Rightarrow \exists\, a, b \in \mathbb{Z}$ s.t. $a^2 \equiv -(1+b^2) \bmod p$

$\Leftrightarrow \exists\, a, b \in \mathbb{Z}$ s.t. $a^2 + (1+b^2) \equiv 0 \bmod p$

$\Leftrightarrow \exists\, a, b \in \mathbb{Z}$ s.t. $a^2 + b^2 + 1 \equiv 0 \bmod p$ □

b) Fix $a, b \in \mathbb{Z}$ as above.
Let $L \subset \mathbb{Z}^4 \subset \mathbb{R}^4$ be the lattice generated by the vectors
$v_1 = (p,0,0,0)$, $v_2 = (0,p,0,0)$, $v_3 = (a,b,1,0)$, $v_4 = (b,-a,0,1)$

Th: $\exists \tilde{k} \in \mathbb{Z}$ s.t. $\|v\|^2 = \tilde{k}p \quad \forall v \in L$

$\forall v \in L$, we can write it as a linear combination of the elements of the basis $\{v_1, v_2, v_3, v_4\}$, that is:
$\forall v \in L$, $\exists\, \alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{Z}$ s.t. $v = \alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + \alpha_4 v_4$.

Therefore, we have that v is the following vector:

$$v = \begin{pmatrix} \alpha_1 p + \alpha_3 a + \alpha_4 b \\ \alpha_2 p + \alpha_3 b - \alpha_4 a \\ \alpha_3 \\ \alpha_4 \end{pmatrix}$$

So, let's compute the value $\|v\|^2$:

$$\begin{aligned}
\|v\|^2 &= (\alpha_1 p + \alpha_3 a + \alpha_4 b)^2 + (\alpha_2 p + \alpha_3 b - \alpha_4 a)^2 + \alpha_3^2 + \alpha_4^2 \\
&= \alpha_1^2 p^2 + \alpha_3^2 a^2 + \alpha_4^2 b^2 + 2\alpha_1\alpha_3 ap + 2\alpha_1\alpha_4 bp + 2\alpha_3\alpha_4 ab + \\
&\quad + \alpha_2^2 p^2 + \alpha_3^2 b^2 + \alpha_4^2 a^2 + 2\alpha_2\alpha_3 bp - 2\alpha_2\alpha_4 ap - 2\alpha_3\alpha_4 ab + \\
&\quad + \alpha_3^2 + \alpha_4^2 \\
&= p^2(\alpha_1^2 + \alpha_2^2) + \alpha_3^2(a^2+b^2) + \alpha_4^2(a^2+b^2) + \alpha_3^2 + \alpha_4^2 + \\
&\quad + 2(\alpha_1\alpha_3 a + \alpha_1\alpha_4 b + \alpha_2\alpha_3 b - \alpha_2\alpha_4 a)p \\
&= p^2(\alpha_1^2 + \alpha_2^2) + (\alpha_3^2 + \alpha_4^2)(a^2+b^2) + (\alpha_3^2 + \alpha_4^2) + \\
&\quad + 2(\alpha_1\alpha_3 a + \alpha_1\alpha_4 b + \alpha_2\alpha_3 b - \alpha_2\alpha_4 a)p \\
&= p^2(\alpha_1^2 + \alpha_2^2) + (\alpha_3^2 + \alpha_4^2)(a^2+b^2+1) + 2(\alpha_1\alpha_3 a + \alpha_1\alpha_4 b + \alpha_2\alpha_3 b - \alpha_2\alpha_4 a)p \\
&\overset{\circledast}{=} p\{(\alpha_1^2 + \alpha_2^2)p + \bar{k}(\alpha_3^2 + \alpha_4^2) + 2(\alpha_1\alpha_3 a + \alpha_1\alpha_4 b + \alpha_2\alpha_3 b - \alpha_2\alpha_4 a)\} \\
&= p\tilde{K}, \quad \exists \tilde{k} \in \mathbb{Z}
\end{aligned}$$

$\circledast$ From part a) we have that there are $a, b \in \mathbb{Z}$ s.t. $a^2+b^2+1 \equiv 0 \pmod p$. We assume that we fix $a, b \in \mathbb{Z}$ s.t. this property is satisfied

$\Rightarrow a^2+b^2+1 = \bar{k}p$ for some $\bar{k} \in \mathbb{Z}$.

$\Rightarrow v$ is a multiple of p for every $v \in L$ $\square$

c) **Th:** $\exists\, u \in L \setminus \{0\}$ of norm $\|u\| < \sqrt{2p}$
$\Rightarrow$ p is the sum of 4 squares of integers

Hint: use Minkowski's theorem

Theorem 9.2.3 (Minkowski). *Let $\mathcal{L} \subset \mathbf{R}^n$ be a lattice. Any convex and centrally symmetric body $S \subset \mathbf{R}^n$ that satisfies $vol(S) > 2^n \operatorname{disc}(\mathcal{L})$ has a non-zero lattice point.*

In our case we have $L = L(\mathcal{B})$ where $\mathcal{B} = \{v_1, v_2, v_3, v_4\}$ with
$v_1 = (p,0,0,0)$, $v_2 = (0,p,0,0)$, $v_3 = (a,b,1,0)$, $v_4 = (b,-a,0,1)$.

We therefore define the basis matrix B as follows:

$$B = \begin{pmatrix} p & 0 & a & b \\ 0 & p & b & -a \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

The discriminant $\operatorname{disc}(L(\mathcal{B}))$ is computed as
$\operatorname{disc}(L(\mathcal{B})) = |\det(B)| = p^2$,
since B is an upper-triangular matrix.

From Gennady Shmonin's notes on Minkowski's theorem and its applications, it seems that a more precise formulation would be the following:

Theorem Let L be a full-dimensional lattice in $\mathbb{R}^n$ and let $S \subseteq \mathbb{R}^n$ be a convex set symmetric about the origin.
Suppose that either
a) $\operatorname{vol}(S) > 2^n \cdot \operatorname{disc}(L(\mathcal{B}))$ or
b) $\operatorname{vol}(S) \geq 2^n \cdot \operatorname{disc}(L(\mathcal{B}))$ and S is compact.
$\Rightarrow \exists$ a couple of non-zero lattice points $\pm z \in S \cap L \setminus \{0\}$.

We want to apply the Theorem to a the open (NON-COMPACT) 4-dimensional ball of radius $\sqrt{2p}$ as our convex symmetric body. The reason for this will be clearer at the end.

So let's consider S to be the open (NON-COMPACT) 4-dimensional ball of radius $\sqrt{2p}$.
We have that $\operatorname{vol}(S) = \frac{\pi^2}{2} R^4 = \frac{\pi^2}{2} 2^2 p^2 = 2\pi^2 p^2$

We notice that indeed $2\pi^2 p^2 = \operatorname{vol}(S) > 2^n \cdot \operatorname{disc}(L(\mathcal{B})) = 2^4 \cdot p^2$
$\Rightarrow$ we can apply Minkowski's theorem with S being NON-COMPACT.

From Minkowski's theorem we have that there is at least one non-zero lattice point u inside the ball S

$\Rightarrow$ such lattice point must be s.t. $\|u\| < \sqrt{2p}$

$\Rightarrow \|u\|^2 < 2p$

But from part (b) we know that for any lattice point v, we have that $\|v\|^2$ is a multiple of p.
For what concerns u, the only multiple of p smaller than $2p$ is p itself

$\Rightarrow \|u\|^2 = p$

We conclude by noticing that if we express $u = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ through its coordinates w.r.t. the basis $\mathcal{B}$, we have that

$$\|u\|^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 \quad \text{with } \alpha_i \in \mathbb{Z} \ \forall i \in \mathbb{Z}$$ (the lattice is a $\mathbb{Z}$-module)

Therefore, we have that

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 = p,$$

proving that p can be indeed expressed as a sum of 4 squares of integers. $\square$