Lecture 19.

We turn our attention back to elliptic curves. Let's consider one more example. The curve E, given by equation $y^2 = x^3 + \underset{\substack{\shortparallel \\ a}}{2}x \underset{\substack{\shortparallel \\ b}}{-1}$ $/\mathbb{F}_5$, is smooth: $D_f = 4 \cdot 2^3 + 27 \cdot (-1)^2 = 59 \equiv 4 \not\equiv 0 \pmod 5$.

The squares modulo 5 are 1 and 4: $1^2 \equiv 4^2 \equiv 1$ and $2^2 \equiv 3^2 \equiv 4 \pmod 5$

Points on E:

$x = 0$: $y^2 = -1 \equiv 4$, so $y \equiv 2$ or $y \equiv 3 \rightsquigarrow$ points $(0,2)$ and $(0,3)$.

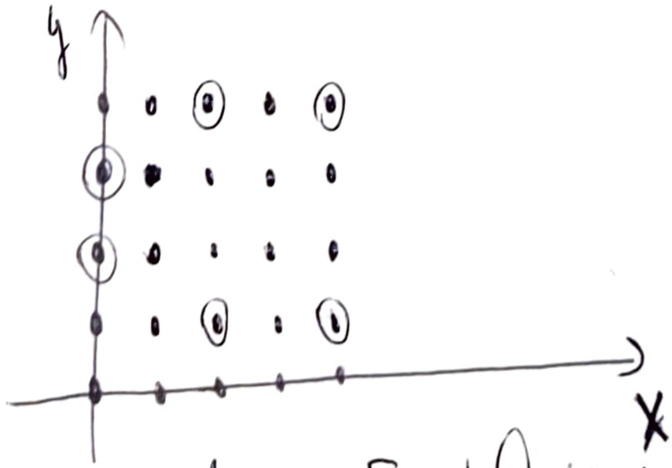
$x = 1$: $y^2 = 1 + 2 - 1 \equiv 2$ ✗ (not a square)

$x = 2$: $y^2 = 8 + 4 - 1 \equiv 1$, so $y \equiv 1$ or $y \equiv 4 \rightsquigarrow$ points $(2,1)$ and $(2,4)$.

$x = 3$: $y^2 = 27 + 6 - 1 = 32 \equiv 2$ ✗ (not a square)

$x = 4$: $y^2 = -1 - 2 - 1 \equiv 1 \rightsquigarrow$ points $(4,1)$ and $(4,4)$

The graphs of E looks as follows:



There are 7 points on E: $\{\underset{\substack{\shortparallel \\ \text{identity}}}{\mathcal{O}}, (0,2), (0,3), (2,1), (2,4), (4,1), (4,4)\}$

Notice that $5 + 1 - 2\sqrt{5} < 7 < 5 + 1 + 2\sqrt{5}$ (as asserted in Hasse's theorem).

As there are 7 points on E, we have that $G(E)$ has 7 elements. It follows immediately (from a lemma below) that $G(E) \simeq \mathbb{Z}/7\mathbb{Z}$.

<u>Lemma.</u> Let $p>1$ be a prime number. Any group of order p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

<u>Proof.</u> Let G be a group of order p and $g \in G$ a nontrivial element. Then the order of g is greater than 1 and divides p, so it has to be equal to p. Therefore, the subgroup generated by g is the whole group G, so G is cyclic.

<u>Rmk.</u> As elements with the same x-coordinate on E add up to identity, we have (without using any formulas)

$$(0,2) \oplus (0,3) = (2,1) \oplus (2,4) = (4,1) \oplus (4,4) = \mathcal{O}.$$

Let's compute $(0,2) \oplus (2,1)$ using the formulas:

$$m = \frac{1-2}{2-0} = 4 \cdot 2^{-1} \equiv 4 \cdot 3 \equiv 2$$

$$\left.\begin{array}{l} x\text{-coordinate} = 2^2 - 0 - 2 \equiv 2 \\ y\text{-coorinate} = -2 - 2(2-0) \equiv 4 \end{array}\right\rangle \quad (0,2) \oplus (2,1) = (2,4).$$

<u>Def-n.</u> A <u>Cayley table</u> (group table) of a finite group G is the table with entries being products of corresponding pairs of elements.

In our example:

Exercise. Fill out the remaining entries.

$\oplus$	ϑ	$(0,2)$	$(0,3)$	$(2,1)$	$(2,4)$	$(4,1)$	$(4,4)$
ϑ	ϑ	ϑ	ϑ	ϑ	ϑ	ϑ	ϑ
$(0,2)$	ϑ		ϑ	$(2,4)$			
$(0,3)$	ϑ	ϑ					
$(2,1)$	ϑ	$(2,4)$			ϑ		
$(2,4)$	ϑ			ϑ			
$(4,1)$	ϑ						ϑ
$(4,4)$	ϑ					ϑ	

Rmk. If G is abelian, then the Cayley table is symmetric.

El Gamal cryptosystem ('classical' and using elliptic curves)

We would like to have a secure message exchange channel (protocol) build on the assumption that the DLP for $(\mathbb{F}_p^\times, \cdot)$ with $p \gg 0$ is extremely hard to solve.

Each participant A creates a private key, k_A $<r$ and publishes the number $g^{k_A} =: A$ (where $g \in \mathbb{F}_p^\times$ is an element known to all participant, so is $r = \mathrm{order}(g)$).

Any two participants A and B create a shared key (if they want to exchange a message): $K_{AB} := AB = g^{k_A k_B} = (g^{k_A})^{k_B} = (g^{k_B})^{k_A}$.

B sends a message $m \in \mathbb{F}_p^\times$ to A via sending the cipher text

$m \cdot K_{AB} =: C$

A retrieves the message as $C \cdot B^{-k_A} = m \cdot K_{AB} \cdot K_{AB}^{-1} = m$.

The version with the group $E/\mathbb{F}_p$ in place of $\mathbb{F}_p^\times$ looks as follows. This time all participants know the number p (prime), curve E, a point $P \in E$ of large prime order r (also known). Each participant chooses a number k_X between 1 and $r-1$ (it is kept in secret) and publishes the point $Q_X = \underbrace{P \oplus \ldots \oplus P}_{k_X}$. The shared key of participants A and B is now $k_A k_B P = k_A Q_B = k_B Q_A =: S^{AB} = (S_x^{AB}, S_y^{AB})$.

A message $m \in \mathbb{F}_p^\times$ $(m = m_1 m_2 \ldots m_s)$ is first broken into two parts: $m_1 m_2 \ldots m_t | m_{t+1} \ldots m_s$ (it is not important where the border line is, say, an end of a logical part will do). Then B sends A two numbers: $L_1 \cdot S_x^{AB}$ and $L_2 S_y^{AB}$, where $L_1 = m_1 \ldots m_t$ and $L_2 = m_{t+1} \ldots m_s$ are the first and second half of the original plaintext message. Then A recovers L_1 as $(L_1 S_x^{AB})(S_x^{AB})^{-1}$ and L_2 as $(L_2 S_y^{AB})(S_y^{AB})^{-1}$.

<u>Rmk.</u> This scheme was proposed by Menezes and Vanstone and is known as MV-ElGamal cryptosystem.

<u>The Double-and-ADD algorithm.</u>

Notice that we need to effectively compute multiples of point P on E. The 'naive' way to add P to itself m types will require $m-1$ operations: $P \oplus P \oplus P \oplus \ldots \oplus P$. Here is a much faster way.

1. Write m in the binary form: $m = m_s 2^s + m_{s-1} 2^{s-1} + \ldots + m_1 2 + m_0$ with $m_i \in \{0,1\}$.
2. Compute $Q_0 = 2^0 P = P$, $Q_1 = Q_0 \oplus Q_0 = 2^1 P$, $Q_2 = Q_1 \oplus Q_1 = 2^2 P$, $\ldots$, $Q_s = Q_{s-1} \oplus Q_{s-1} = 2^s P$
3. $mP = \bigoplus_{m_j = 1} Q_j$

<u>Example</u>. Find 67P.

1. $69 = 64 + 4 + 1 = 2^6 + 2^2 + 1$.
2. Find $Q_1, Q_2, Q_3, Q_4, Q_5, Q_6 \to 6$ operations
3. $69P = Q_6 \oplus Q_2 \oplus P \to 2$ operations

8 Vs 68

'stupid' addition

Shor's algorithm for DLP with $G = G(E/\mathbb{F}_p)$.

Let G be a group of points on an elliptic curve E defined over finite field $\mathbb{F}_p$.

Given: p, eq-n $y^2 = x^3 + ax + b$ of E, a point P on E and its order r. together with another point $Q = kP := \underbrace{P \oplus \ldots \oplus P}_{k}$.

Goal: find k.

As before, we reformulate this problem as an instance of a hidden subgroup problem.

Let $\mathbb{Z}/r\mathbb{Z} = \langle P \rangle \subset G(E/\mathbb{F}_p)$ be the cyclic subgroup generated by P (we simplify identify P with $1 \in \mathbb{Z}/r\mathbb{Z}$).

Set $K := \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ and $S := \mathbb{Z}/r\mathbb{Z}$ with

$f: K \to S$ given by $f(a,b) := a - bk \pmod r$ (or $aP - bQ \in E$).

Then $H := \{(a,b) \mid f(a,b) = 0\}$ is the hidden subgroup and the knowledge of H allows to find k (see previous lectures).

We will $\underbrace{\text{use}}_{\text{show how to}}$ (an instance of) 'Shor's algorithm to 'find' (some info on) H.

① Prepare the generic state

$$\frac{1}{r} \sum_{0 \le a, b \le r-1} |a\rangle |b\rangle |aP\rangle |bQ\rangle |0\rangle$$

② Apply the oracle O_f to get $\displaystyle \frac{1}{r} \sum_{1 \le a, b \le r-1} |a\rangle |b\rangle |aP\rangle |bQ\rangle \overset{|a-bk\rangle}{\overset{\shortparallel}{|aP-bQ\rangle}}$

③ Measure the last register: the outcome will be some $t = a' - b'k$ and the state will collapse to

$$\frac{1}{\sqrt{r}} \sum_{a,b:\, a-bk \equiv t \pmod r} |a\rangle|b\rangle|aP\rangle|bQ\rangle$$

④ Apply the QFT for the group $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ (as we discussed, it is the tensor product of two copies of QFT for $\mathbb{Z}/r\mathbb{Z}$):

$$\frac{1}{\sqrt{r}} \sum_{\substack{a,b \\ a-bk\equiv t}} |a\rangle|b\rangle|aP\rangle|bQ\rangle \xrightarrow{QFT} \frac{1}{r^{3/2}} \sum_{\substack{a,b \\ a-bk\equiv t}} \sum_{j=0}^{r-1} \omega^{aj}|j\rangle|jP\rangle \sum_{s=0}^{r-1} \omega^{bs}|s\rangle|sQ\rangle =$$

$$= \frac{1}{r^{3/2}} \sum_{j=0}^{r-1} \sum_{s=0}^{r-1} \sum_{\substack{a,b \\ a-bk\equiv t}} \omega^{aj+bs} |j\rangle|s\rangle|jP\rangle|sQ\rangle = \frac{1}{r^{3/2}} \sum_{j=0}^{r-1} \sum_{s=0}^{r-1} \sum_{b=0}^{r-1} \omega^{(bk+t)j+bs} |\ldots\rangle$$

$|j\rangle|s\rangle|jP\rangle|sQ\rangle.$

Let's simplify the expression $\sum_{b=0}^{r-1} \omega^{(bk+t)j+bs}$ (recall that $\omega = e^{2\pi i/r}$):

$$\sum_{b=0}^{r-1} \omega^{(bk+t)j+bs} = \omega^{tj} \sum_{b=0}^{r-1} \omega^{b(kj+s)} = \begin{cases} r\omega^{tj}, & kj+s \equiv 0 \pmod r \\ 0, & \text{otherwise.} \end{cases}$$

So our current state can be written as

$$\frac{1}{r^{3/2}} \sum_{\substack{s,j \\ kj+s\equiv 0}} r\omega^{tj} |j\rangle|s\rangle|jP\rangle|sQ\rangle = \frac{1}{\sqrt{r}} \sum_{\substack{s,j \\ kj+s\equiv 0}} \omega^{tj} |j\rangle|s\rangle|jP\rangle|sQ\rangle$$

(5) Measure the remaining registers, giving rise to some l, u, lP, uQ with $kl + u \equiv 0 \pmod r$.

Then we find k as $k \equiv -ul^{-1} \pmod r$.

Rmk. Usually r is chosen to be prime, but even if not, the odds for $\gcd(l, r) \neq 1$ are very low.