5. Projective plane curves and Bézout's thm:

5.1 Definitions:

As in the affine case, we want to allow multiple components

Def: Two non-const. forms $F, G \in k[X,Y,Z]$ are equivalent if $\exists \lambda \in K$ s.t. $F = \lambda \cdot G$.

- A proj. plane curve is an equivalence class of forms. The degree of proj plane curve is the degree of a form representing it.

As before we'll write $F \subset \mathbb{P}^2$ instead of $V(F)$ for a proj. plane curve defined by a form F.

- Curves of degree 1, 2, 3, 4 are called lines, conics (or quadrics), cubics and quartics.
- Components and their multiplicities are defined as in the affine case.
- $\mathcal{O}_P(F)$ and $k(F)$ are defined as in Chapter 3. If $P=[X:Y:1]$ then $\mathcal{O}_P(F) = \mathcal{O}_{(X,Y)}(F_*)$ where $F_*(X,Y) = F(X,Y,1)$ is the dehomogenization of F.
- The multiplicity $m_P(F)$ of F at P for F irred. is defined as $m_P(F) = \dim_k\left(\mathfrak{m}_P^n(V)/\mathfrak{m}_P^{n+1}(V)\right)$ for $n \gg 0$.

If $F = \prod_i F_i^{e_i}$ then $m_P(F) := \sum_i e_i \cdot m_P(F_i)$.

If $P=[X:Y:1] \in U_\infty$ then $m_P(F) = m_P(F_*)$ by Theorem 4.1.

- If $P \in F$ is a simple point (i.e. $m_P(F)=1$) and F is irred.

· If $P \in F$ is a simple point (i.e. $m_P(F) = 1$) and F is irred. then $\mathcal{O}_P(F)$ is a DVR by Corollary 4.4. We write ord_P^F for the corresp. order function on $K(F)$.

· If $P = [X:Y:1]$ and F, G are proj. plane curves, we define

$$I(P, F \cap G) = I((x,y), F_* \cap G_*) := \dim_k\left(\mathcal{O}_{(x,y)}\mathbb{A}^2 / (F_*, G_*)\right)$$

If $P \notin U_\infty$ we may choose any other dehomog.

Rmk: We'd like to say $I(P, F \cap G) = \dim_k(\mathcal{O}_P(\mathbb{P}^2)/(F,G))$ but this doesn't quite makes sense since F, G don't define elements in $\mathcal{O}_P(\mathbb{P}^2)$. However if L is any line not containing P, then $F/L^{\deg F} \in \mathcal{O}_P(\mathbb{P}^2)$ and if L' is another such line then $F/L^{\deg F}$ and $F/L'^{\deg F}$ differ by the unit $(L'/L)^{\deg F}$ in $\mathcal{O}_P(\mathbb{P}^2)$. Hence by abuse of notation we may write $F \in \mathcal{O}_P(\mathbb{P}^2)$ for the class of $F/L^{\deg F}$, which is well-def up to a unit and then $\dim_k(\mathcal{O}_P(\mathbb{P}^2)/(F,G)) = I(P, F \cap G)$.
l.p. $I(P, F \cap G)$ doesn't depend on the dehomog.

Def: A line is tangent to a curve F at P if
$I(P, F \cap L) > m_P(F)$.

· P is an ordinary multiple point of F if there are $m_P(F)$ distinct tangents to F at P.

5.2 Bézout's Theorem.

Thm 5.1 (Bézout's thm): Let F, G be proj. plane curves of degree m and n respectively. Assume F and G have no common components. Then

$$\sum I(P, F \cap G) = m \cdot n$$

$$\sum_{P \in F \cap G} I(P, F \cap G) = m \cdot n$$

Before we go to the proof, let's see some immediate consequences:

Corollary 5.2: If F, G have no common component, then

$$\sum_{P \in F \cap G} m_P(F) \cdot m_P(G) \leq \deg(F) \cdot \deg(G)$$

pf: We have (Thm 4.5 5))

$$\deg(F) \cdot \deg(G) = \sum_{P \in F \cap G} I(P, F \cap G) \geq \sum_{P \in F \cap G} m_P(F)\, m_P(G)$$

□

Corollary 5.3: If F and G meet in $\deg(F) \cdot \deg(G)$ points, then all these points are simple on F and on G.

Corollary 5.4: If two curves of degree m and n have more than $m \cdot n$ points in common, then they have a common component.

You'll see some very concrete consequences in the exercises for example a curve of degree n can have at most $\frac{n(n-1)}{2}$ multiple points.

pf of Bézout: No common components $\Rightarrow |F \cap G| < \infty$. Using a proj. change of coordinates we may assume that no point of $F \cap G$ lies on the line at $\infty \leftrightarrow \{Z = 0\}$.

Then $\sum I(\quad) = \sum I(P, F \cap G) = \quad$ [illegible]

that no point of $F \cap G$ lies on the line at $\infty \leftrightarrow \{Z=0\}$.

Then $\sum_{P \in F \cap G} I(P, F \cap G) = \sum_{P \in F_* \cap G_*} I(P, F_* \cap G_*) = \dim_k k[X,Y]/(F_*, G_*)$

(Thm 4.5, 3)

Set $\Gamma = k[X,Y,Z]/(F,G)$, $\Gamma_* = k[X,Y]/(F_*, G_*)$, $R = k[X,Y,Z]$

We'll study Γ_* through the map

$$h : \Gamma \longrightarrow \Gamma_*$$
$$\overline{H} \mapsto \overline{H_*}$$

Set $R_d = \{H \in R \mid \deg H = d\} \cup \{0\}$, a k-vect. sp.

and $\Gamma_d = \{\overline{H} \in \Gamma \mid \deg H = d\} \cup \{0\}$

Claim 1: $\dim_k \Gamma_d = m \cdot n$ for all $d \geq m+n$

pf: Let $\pi : R \to \Gamma$ be the quotient map. Since F, G have no common factors we have an exact seq.

$$0 \longrightarrow R \xrightarrow{\psi} R \times R \xrightarrow{\varphi} R \xrightarrow{\pi} \Gamma \longrightarrow 0$$
$$(A,B) \mapsto A \cdot F + B \cdot G$$
$$C \mapsto (C \cdot G, -C \cdot F)$$

Restricting to a given degree we get

$$0 \longrightarrow R_{d-m-n} \longrightarrow R_{d-m} \times R_{d-n} \longrightarrow R_d \longrightarrow \Gamma_d \longrightarrow 0$$

Since $\dim R_k = \frac{(k+1)(k+2)}{2}$ $\Rightarrow \dim_k \Gamma_d = m \cdot n$. $\square$

Claim 2: The map $\alpha : \Gamma \to \Gamma$, $\overline{H} \mapsto \overline{Z \cdot H}$ is injective

In part $\alpha_{|\Gamma_d} : \Gamma_d \to \Gamma_{d+1}$ is an iso. for $d \geq m+n$.

4th part $\alpha_{|\Gamma_d}: \Gamma_d \to \Gamma_{d+1}$ is an iso. for $d \geq m+n$.

pf: Assume $\overline{z \cdot H} = 0$, then $z \cdot H = AF + B \cdot G$

Let $A_0, B_0, F_0, G_0 \in k[X,Y]$ for $A[X,Y,0]$ etc. Now $F \cap G \cap \{z=0\} = \emptyset$,

$F_0 \cap G_0 = F \cap G \cap \{z=0\} = \emptyset$.

$\rightsquigarrow$ F_0 and G_0 have no common component

$A_0 F_0 = -B_0 G_0 \Rightarrow \exists\, C \in k[X,Y]$ s.t. $B_0 = F_0 \cdot C$

and $-G_0 \cdot C = A_0$. Set $A' = A + GC$ and $B' = B - FC$.

Then $A'_0 = A_0 + G_0 \cdot C = 0 = B'_0 \rightsquigarrow z \mid A', z \mid B'$

$\rightsquigarrow H = \left(\frac{A+GC}{z}\right) \cdot F + \left(\frac{B-FC}{z}\right) \cdot G \rightsquigarrow \overline{H} = 0 \rightsquigarrow \alpha$ is injective.

Claim 3: $h_{|\Gamma_d}: \Gamma_d \to \Gamma_*$ is an isom. of K-v. sp. for $d \geq m+n$

i.p. $\dim_K(\Gamma_*) = m \cdot n$.

pf: Let $\overline{A}_1, \dots, \overline{A}_{m \cdot n}$ be a basis of Γ_d.

- Then $\{h(\overline{A}_i)\}_i = \{\overline{A}_{i*}\}_i$ generates Γ_*:

  Let $\overline{H} \in \Gamma_*$ and some $N > 0$ s.t. $z^N H^* = z^N H\left(\frac{X}{z}, \frac{Y}{z}\right)$ is a form of degree $d' \geq d$. $\rightsquigarrow \overline{z^N H^*} \in \Gamma_{d'} \overset{\text{claim 2}}{\cong} \Gamma_d$

  $\rightsquigarrow \overline{z^N H^*} = \sum_{i=1}^{m \cdot n} \lambda_i \overline{z^{d'-d} A_i}$

  $\rightsquigarrow \overline{H} = \left(\overline{z^N H^*}\right)_* = \sum_{i=1}^{m \cdot n} \lambda_i \overline{A}_{i*}$.

- $\{\overline{A}_{i*}\}_i$ are lin independent: $\sum_{i=1}^{m \cdot n}$

- $\{A_{i,*}\}_i$ are lin independent:

Assume $\sum_{i=1}^{m\cdot n} \lambda_i \overline{A_{i,*}} = 0 \iff \sum_{i=1}^{m\cdot n} \lambda_i \lambda_{i,*} = A F_* + B \cdot G_*$

Applying $(\,)^*$ we see that $\exists\, a,b,c \geq 0$ s.t.

$$z^a \sum \lambda_i \lambda_i' = z^b A^* F + z^c B^* G.$$

$\rightsquigarrow \sum \lambda_i \overline{z^a A_i} = 0$ in Γ_{d+a} $\overset{\text{claim 2}}{\rightsquigarrow}$ $\lambda_i = 0\ \forall i$. $\overset{\text{claim 3}}{\square}$ thm. $\square$

5.3 Applications to incidence geometry

Theorem 5.5 (Cayley-Bacharach): Let F_1, F_2 be two proj. cubics intersecting in exactly 9 different points $A_1, \dots, A_9 \in \mathbb{P}^2$. If G is another cubic w/ $A_1, \dots, A_8 \in G$, then G is a linear combination of F_1 and F_2, i.p. $A_9 \in G$.

pf: 1) No 4 points of $F_1 \cap F_2 = \{A_1, \dots, A_9\}$ are colinear. Otherwise the line L containing those 4 points would be a component of F_1 and F_2 by Cor 5.4. But then $|F_1 \cap F_2| > L$ ↯.

2) By the same argument no 7 ($> 2 \cdot 3$) points of $F_1 \cap F_2$ lie on a quadric.

3) Any 5 points in $F_1 \cap F_2$ define a unique quadric:

Existence: A general quadric in $\mathbb{P}^2$ has the form

$$a_1 X^2 + a_2 Y^2 + a_3 Z^3 + a_4 XY + a_5 YZ + a_6 ZX.$$

$$a_1X + a_2Y + a_3Z + a_4XY + a_5YZ + a_6ZX.$$

The 5 pts will give 5 linear conditions for $a_1, \dots, a_6$
$\rightsquigarrow \exists$ non-trivial solution by lin. alg.

Uniqueness: Assume Q_1, Q_2 are two quadrics containing the 5 pts. Then by cor. 5.4, they share a component, that must be a line L (otherwise $Q_1 = Q_2$).
By 1) the line L contains at most three of the 5 pts.
But then $\frac{Q_1}{L}, \frac{Q_2}{L}$ are lines that pass through the two remaining points $\rightarrow Q_1/L = Q_2/L \Rightarrow Q_1 = Q_2$

4) No 3 points in $\{A_1, \dots, A_8\}$ are colinear:
Assume A_1, A_2, A_3 lie on a line L. Then $A_4, \dots, A_8$ do not lie on L by 1) and $\exists!$ quadric Q passing through $A_4, \dots, A_8$ by 3).
Let $B \in L \setminus \{A_1, A_2, A_3\}$ and $C \in \mathbb{P}^2 \setminus \{L, Q\}$.
By lin. alg. $\exists \alpha, \beta, \gamma \in K$, not all $= 0$, s.t.

$$H := \alpha F_1 + \beta F_2 + \gamma G$$

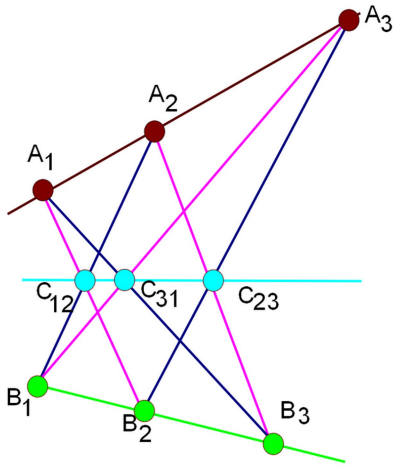
vanishes on B and C, and $H \neq 0$ (otherwise we're done).
Then H vanishes on $A_1, A_2, A_3, B \overset{5.4}{\rightsquigarrow} L \mid H$
and the quadric H/L vanishes on $A_4, \dots, A_8 \overset{3)}{\rightsquigarrow} H/L = Q$.
$\rightsquigarrow H = L \cdot Q$ but $L(C) \cdot Q(C) \neq 0$ $\lightning$.

5) No 6 points on $\{A_1, \dots, A_8\}$ lie on a quadric (Exercise)

6) End of pf: Let l be the line through A_1 and A_2

6) End of pf: Let L be the line through A_1, A_2 and Q the unique quadric through $A_3, \dots, A_7$.
Pick $B_1 C \in L \setminus \{A_1, A_2\}$ and let $H = \alpha F_1 + \beta \cdot F_2 + \gamma \cdot G$ s.t. $B_1, C \in H$ and assume $H \neq 0$.
Then $A_1, A_2, B_1, C \in H \cap L \rightsquigarrow L \mid H$ and $A_3, \dots, A_7 \in H/L$ (4)
$\rightsquigarrow H/L = Q$. But $A_8 \notin L \cdot Q = H$ $\lightning$ $\rightsquigarrow H = 0$
(↖ 4), 5)) □

Corollary 5.6 (Pappus' thm): Let $L_1, L_2 \subset \mathbb{P}^2$ be two distinct lines. Let $A_1, A_2, A_3 \in L_1 \setminus L_2$ and $B_1, B_2, B_3 \in L_2 \setminus L_1$.
Let C_{ij} be the intersection of the lines $\overline{A_i B_j}$ and $\overline{A_j B_i}$ for $ij = 12, 23$ and 31.
Then C_{12}, C_{23} and C_{31} are colinear.



Rmk: Typically this theorem is stated in $\mathbb{R}^2$. But we may just consider the equations of the real lines in $\mathbb{C}^2$, homogenize, and then apply the thm above.

pf: Let F_1 be the product of the purple lines
- F_2 ∥ blue lines
- G ∥ L_1, L_2 and $\overline{C_{12} C_{31}}$

These are all cubics, $|F_1 \cap F_2| = 9$ (if two of the C_{ij}'s

These are all cubics, $|F_1 \cap F_2| = 9$ (if two of the C_{ij}'s agree, the thm is trivial) and G passes through 8 of the 9 points $\overset{5.5}{\rightsquigarrow} C_{23} \in G$. But $C_{23} \nsubseteq L_1 \cdot L_2 \rightsquigarrow C_{23} \in \overline{C_{12} C_{23}}$ □

5.4 Elliptic curves:

We have seen in Ex 6.5, that $F \subset \mathbb{P}^2$ of deg 2 and irred ($\Leftrightarrow$ non-sing) is isomorphic to $\mathbb{P}^1$.
Elliptic curves are the next "simplest" case i.e. deg = 3:

Def: An elliptic curve (E, O) is a non-singular (hence irred by Ex. 11.1) cubic $E \subset \mathbb{P}^2$ together with a point $O \in E$.

Somewhat unexpected one can define a commutative group law on E with O as the neutral element.

Define a map $\varphi : E \times E \to E$ as follows:

$\varphi(A, B) \in E$ is the unique third intersection point of the line $\overline{AB}$ with E if $A \neq B$, or of the tangent at A with E if $A = B$ (the tangent is unique since E is non-singular).

We then define the addition as

$$A + B := \varphi(O, \varphi(A, B)).$$

Theorem 5.7: $(E, +, O)$ is a commutative group.

pf: clearly $A + B = B + A$.

$O + A = A$: Let $C = \varphi(O, A)$. Then the line through O and

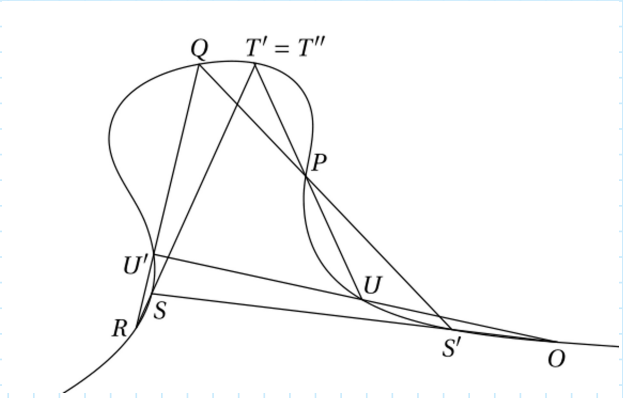
$O+A=A$: Let $C=\varphi(0,A)$. Then the line through O and C intersects E in A $\rightsquigarrow$ $O+A=\varphi(0,\varphi(0,A))=A$

Inverse: To define the inverse of $A\in E$, let $P=\varphi(0,0)$ and set $-A=\varphi(A,P)$. Then

$$A+(-A)=\varphi(0,\varphi(A,\varphi(A,P)))=\varphi(0,P)=0.$$

Associativity: Let $P,Q,R\in E$. We want

$$(P+Q)+R=P+(Q+R)$$



Set $\varphi(P,Q)=S'$ and $P+Q=S$

and $\varphi(Q,R)=U'$ and $Q+R=U$

In order to show $S+R=P+U$

it's enough to show $T':=\varphi(R,S)=\varphi(P,U)=:T''$

(Assume that no points collide for simplicity)

Let F be the product of the three lines $\overline{QP}$, $\overline{UU'}$, $\overline{RS}$

Then F and E intersect in 9 distinct points.

The product G of the other three lines $\overline{QR}$, $\overline{SS'}$, $\overline{PU}$ contains 8 of these 9 points (all but T') and hence by the Thm of Cayley-Bacharach also T'.

Since $|G\cap E|=9$ we deduce that $T=T''$ □

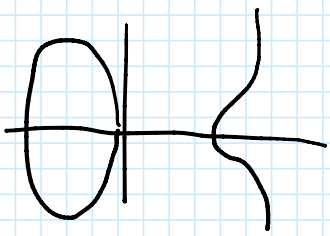
Let's see a bit more concretely what these curves are.

Lemma 5.8 Any elliptic curve is isomorphic to a curve with equation $Y^2Z - X^3 - aXZ^2 - bZ^3$, $O=[0:1:0]$ (♣)
where $a,b \in k$ s.t $4a^3+27b^2 \neq 0$.

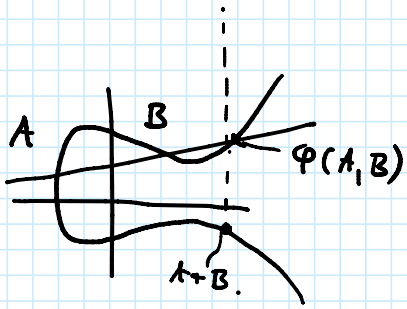
Sketch of pf: Some clever change of coordinates to get (♣). The condition $4a^3+27b^2 \neq 0$ is equivalent to not having a multiple point. □

Rmk: Notice that O is the only point w/ $Z=0$.
Thus one usually sometimes thinks of (♣) as the affine plane curve $Y^2 - X^3 - aX - b$ together w/ a point O at ∞.
• (♣) is called the **Weierstrass normal form** of (E,O)

Exple:

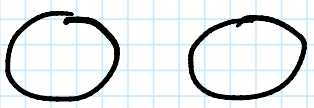


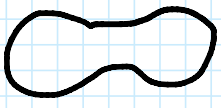
$y^2 = x^3 - x$



$y^2 = x^3 - x + 1$

Rmk: If we add the point O in these pictures we get a compactification that looks as follows





Those are 2 different section of a torus 
In fact one can show that for $k=\mathbb{C}$
E is homeomorphic to a torus $T = S^1 \times S^1$.

Thm: F of deg d, $g(F) = \frac{(d-1)(d-2)}{2}$

Exples: $d=1$ F is a line $\Rightarrow$ $F \simeq \mathbb{P}^1$

$\mathbb{C}\mathbb{P}^1 \simeq$  as topol spaces genus$(F)=0$.

· $d=2$: We also saw in the exercices, that $F \simeq \mathbb{P}^1$.

genus$(F) = 0$.

· $d=3$: genus$(F)=1$ $\rightsquigarrow$ $F \simeq$  $\rightarrow$ elliptic curves.

Let's try to understand this thm:

Assume $[1:0:0] \notin F \Leftrightarrow F(X,Y,Z) = X^d + \dots$

Thus we have a morphism

$$\pi : F \longrightarrow \mathbb{P}^1$$

$$(X:Y:Z) \longmapsto (Y:Z)$$

$\pi^{-1}(X_0:Z_0) = \{F(X,Y_0,Z_0)=0\}$ so $|\pi^{-1}(Y_0:Z_0)| = d$ unless

$F(X,Y_0,Z_0)$ has a multiple point.

$\Updownarrow$

$\frac{\partial F}{\partial X} \cap F \neq \emptyset$.

By moving the eq's a bit, we can assume that

$F(X,Y_0,Z_0)$ has no zero of multiplicity 3

i.e. $\frac{\partial F}{\partial X^2} \cap \frac{\partial F}{\partial X} \cap F = \emptyset$ (3 eq's in $\mathbb{P}^2$)

Therfore we have $\forall P \in \frac{\partial F}{\partial X} \cap F \subset \mathbb{P}^2$, $I(P, \frac{\partial F}{\partial X} \cap F) = 1$:

Indeed we can assume the tangent (i.e. $P=(0:0:1) \in U_\infty$)

Indeed we can compute the tangents (say $P=(0:0:1)\in C_\infty$)

Let $F'=F(X,Y,1)$. Then $\neq 0$

Tangent at F': $\frac{\partial F'}{\partial x}(0,0)\cdot X+\frac{\partial F'}{\partial y}(0,0)\cdot Y$

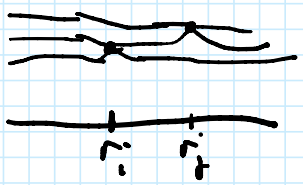
$\parallel$ $\frac{\partial F'}{\partial x}$: $\frac{\partial F'}{\partial x^2}(0,0)\cdot X+\frac{\partial F'}{\partial x\partial y}(0,0)\cdot Y$ $\neq 0$

Tangents are different

I) $\Rightarrow I_P\left(P, \frac{\partial F}{\partial x}\cap F\right)=1$.

Bezout $\Rightarrow \left|\frac{\partial F}{\partial y}\cap F\right| = d(d-1)$.

Let $r_1,\dots,r_{d(d-1)}$ be the images under π of these multiple points.



So the fibers of π have cardinality d except

$|\pi^{-1}(r_i)| = d-1$.

This determines the genus of F:

Choose a cell-decomposition of $\mathbb{CP}^2$ containing the r_i's as vertices:

$\sigma_0 = \#$ points/vertices

$\sigma_1 = \#$ 1-cells

$\sigma_2 = \#$ 2-cells

Euler char. $\chi(\mathbb{CP}^1)=\sigma_2-\sigma_1+\sigma_0=2$.

Pulling back this decomp. under π we get one for F and $\sigma_{2,F}=d\cdot\sigma_2$, $\sigma_{1,F}=d\cdot\sigma_1$, $\sigma_0 = d\cdot\sigma_0 - d(d-1)$

$\rightarrow \chi(F) = \sigma_{2,F}-\sigma_{1,F}+\sigma_{0,F} = 2\cdot d - d(d-1) = 3d-d^2$.

$g(F) = 2-\chi(F) = \frac{2-3d+d^2}{} = (d-1)(d-2)$

$$\rightsquigarrow \text{genus}(F) = \frac{2-\chi(F)}{2} = \frac{2-3d+d^2}{2} = \frac{(d-1)(d-2)}{2}.$$

Applications of elliptic curves:

Fermat's last theorem:

$a^n + b^n = c^n$ has no non-trivial integer solution for $n > 2$. (If $n = p$ prime is enough)

Frey's idea: Consider the elliptic curve

$$y^2 = x(x-a^p)(x+b^p)$$

where $a^p + b^p = c^p$.

If this curve exists it must have some strange arithmetic properties, and Wiles ultimately showed that no elliptic curve can have these (Taniyama-Shimura conj.)

- Elliptic curve cryptography

Lenstra's Algorithm for integer factorization

Given an integer $n \in \mathbb{Z}$, there is currently no algorithm known, that computes the prime factors of n in polynomial time (There is if one allows quantum computers).

Lenstra's alg. (1987) is among the fastest sub-

Lenstra's alg. (1987) is among the fastest sub-exponential algorithms known ($< O\left((1+\varepsilon)^{\ln(n)}\right)^{c}\ \forall \varepsilon > 0$)

The basic idea is to compute $\gcd(a,n)$ for a varying in a finite subset of $\mathbb{Z}$, and hope to find an answer $\neq 1$. If the subset is "well chosen", this turns out to be efficient.

Pollard's $(p-1)$-method:

- Choose a random $a \in \mathbb{Z}/n\mathbb{Z}$ and $k \in \mathbb{N}$ with many small prime divisors (e.g. $k = \mathrm{lcm}(1,\dots,b)$ for some $b \in \mathbb{N}$).

Then compute $a^k \bmod (n)$ and $\gcd(a^k - 1, n)$

This works well if n has a prime-divisor p s.t. $p-1$ is a product of small primes i.e. if $p-1 \mid k$. If we further assume $p \nmid a$, then by Fermat's thm

$$p \mid a^k - 1 \quad \text{and} \quad p \mid \gcd(a^k - 1, n)$$ and we can detect p by this method.

In order to explain Lenstra's idea we have to believe that everything we learned about elliptic curves (group law, Weierstrass eq.) over an alg. closed field k, also holds true over $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$.

If we believe this we can basically just replace the group $(\mathbb{Z}/p\mathbb{Z})^*$ above by an elliptic curve / $\mathbb{Z}/p\mathbb{Z}$.

Lenstra's algorithm

Given $n>1$ choose the following:

- A random elliptic curve over $\mathbb{Z}/n\mathbb{Z}$ i.e. an equation
$$(*) \quad Y^2Z = X^3 + aXZ^2 + bZ^3, \quad 0 = [0:1:0].$$
where $a,b \in \mathbb{Z}/n\mathbb{Z}$, $4a^3+27b^2 \neq 0$.
- An integer k with many small prime divisors
- A random point e on E over $\mathbb{Z}/n\mathbb{Z}$ i.e. $x,y,z \in \mathbb{Z}/n\mathbb{Z}$, not all $=0$, satisfying $(*)$

Rmk: x,y,z above define a point $[x:y:z] \in \mathbb{P}^2(\mathbb{Z}/n\mathbb{Z})$ This homog. coordinates are well-def. up to multiplication by units, i.e. elements in $(\mathbb{Z}/n\mathbb{Z})^*$.

Now compute $k \cdot e := \underbrace{e+e+\dots+e}_{k\text{-times}}$ and the gcd of it's z-coordinate with n. (By the rmk is well-def). If it's $\neq 1$ we have found a divisor of n.

Why does it work: For $p \mid n$ write $E(\mathbb{Z}/p\mathbb{Z})$ for the set of solutions to $(*)$ w/ $x,y,z \in \mathbb{Z}/p\mathbb{Z}$. It's a finite group and it's size satisfies $p+1-2\sqrt{p} < |E(\mathbb{Z}/p\mathbb{Z})| < p+1+2\sqrt{p}$.

group and it's size satisfies $p+1-2\sqrt{p} < |E(\mathbb{Z}/p\mathbb{Z})| < p+1+2\sqrt{p}$.

Now assume $\exists p \mid n$ s.t. $|E(\mathbb{Z}/p\mathbb{Z})| \mid K$

($e \equiv [0:1:0] \bmod p$.)

Then $K \cdot e = 0$ in $E(\mathbb{Z}/p\mathbb{Z})$ $\Leftrightarrow$ $Ke \equiv [0:1:0] \bmod p$

$\Leftrightarrow$ z-coord of Ke is divisible by r.

In other words, the algorithm works if n has a prime divisor p s.t. $|E(\mathbb{Z}/p\mathbb{Z})|$ is a product of small primes. Since we are free to choose E (or in practice several E's) this works quite well!