Lecture 14

Jose Capco (jcapco@risc.jku.at)

Recall that a finitely generated abelian group $(G,+)$ is an abelian group with a finitely many generators i.e. $g_1,\dots,g_k$ such that for all $g\in G$ there are $n_1,\dots,n_k\in\mathbb{Z}$ with

$$g=\sum_{i=1}^{k} n_i g_i$$

We know from the fundamental theorem of finitely generated abelian groups that a finitely generated abelian group $(G,+)$ can be written as

$$G=H\oplus \mathrm{Tor}(G)$$

where H is a free group, i.e. $H\cong\mathbb{Z}^r$ for some $r\in\mathbb{N}$. The number r is called the *rank* of the group G.

Last session we said that the Mordell-Weil Theorem states that $E(\mathbb{Q})$ is a finitely generated abelian group. We will not prove this result but we will give idea of how the proof is accomplished. To prove the Mordell-Weil Theorem one first proves the so-called Weak-Mordell-Theorem:

Weak Mordell Theorem. Let E be an elliptic curve over $\mathbb{Q}$, then the quotient $E/2E$ is finite.

Proof Idea. First assume $E: y^2=x^3+ax+b=(x-e_1)(x-e_2)(x-e_3)$ for some algebraic numbers $e_1,e_2,e_3\in\mathbb{Q}$. One then defines the field $K:=\mathbb{Q}(e_1,e_2,e_3)$ and proves that $E(K)/2E(K)$ is finite implies that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. One uses a tool that makes it easier to prove that $E(K)/2E(K)$ is finite namely one proves that the map

$$\begin{array}{rccl}
\phi: & (E(K),+) & \longrightarrow & (K^*/(K^*)^2,*)^3 \\
& O & \mapsto & (1,1,1) \\
& (x,y) & \mapsto & (x-e_1,x-e_2,x-e_3) \quad (y\neq 0) \\
& (e_1,0) & \mapsto & ((e_1-e_2)(e_1-e_3),e_1-e_2,e_1-e_3) \\
& (e_2,0) & \mapsto & (e_2-e_1,(e_2-e_1)(e_2-e_3),e_2-e_3) \\
& (e_3,0) & \mapsto & (e_3-e_1,e_3-e_2,(e_3-e_1)(e_3-e_2))
\end{array}$$

is a group homomorphism and has a finite image and a kernel that is $2E(K)$ and this prove the theorem. □

Note that for an abelian group $(G,+)$, $G/2G$ being finite does not necessarily imply that G is a finitely generated. A counterexample is $(G,+)=(\mathbb{Q},+)$ or $(G,+)=(\mathbb{R},+)$, in this case $G/2G$ is just trivial but G is not finitely generated. So, there is more into elliptic curves that allows us to conclude finite generation from the Weak Mordell Theorem.

The remaining tools needed to prove the Mordell-Weil Theorem relies on the theory of heights. We give some motivation on theory without much rigorous proof:

- We observe that for any $N\in\mathbb{N}$ the set

$$\{n\in\mathbb{Z}\,:\,|n|\leq N\}$$

is finite

- The above is not true if we replace $\mathbb{Z}$ by $\mathbb{Q}$, namely

$$\{q\in\mathbb{Q}\,:\,|q|\leq N\}$$

is infinite. This motivates the idea of (logarithmic) height of rational numbers i.e. we want to order increasing finite subsets of $\mathbb{Q}$ by heights. Let $q\in\mathbb{Q}$ then we can write $q=a/b$ for some unique $a\in\mathbb{Z},b\in\mathbb{N}$ with $\gcd(a,b)=1$ and define its height to be

$$h(q):=\ln(\max\{|a|,|b|\})$$

With this we now get a finite set

$$\{q\in\mathbb{Q}\,:\,h(q)\leq N\}$$

• This idea is used also for points $P \in E(\mathbb{Q})$ of an elliptic curve E over $\mathbb{Q}$. Namely: $h(P) := h(x_P)$ if $P \neq O$ and $h(O) = 0$. But this is often replaced by another height function with better properties called the *Néron-Tate height* or the *canonical height* denoted by $\hat{h}$:

$$\hat{h}(P) := \lim_{n\to\infty} \frac{1}{2^{2n+1}} h(2^n P)$$

Of course one has to show that this limit always exists. One nice property of this height function is that $\hat{h}(P) = 0$ iff $P \in \mathrm{Tor}(E)$ and we may use this in the last lecture when discussing ranks. In any case one also has

$$\{P \in E(\mathbb{Q}) \,:\, \hat{h}(P) \leq N\}$$

is finite.

The above canonical height function will allow one to prove the Mordell-Weil theorem by counting points in an elliptic curve $E/\mathbb{Q}$:

Idea of Proof of Mordell-Weil Theorem. Let E be the elliptic curve over $\mathbb{Q}$ and let $\{R_1, \ldots, R_n\} \subset E$ be a finite set of points that represent elements in the finite group $E/2E$. Define

$$C := \max\{\hat{h}(R_i) \,:\, i = 1, \ldots, n\}$$

and consider the finite set

$$\{P \in E : \hat{h}(P) \leq C\}$$

In a final step one uses the properties of $\hat{h}$ to show that the above set of points generates E. □

We now illustrate some nice applications of elliptic curves over $\mathbb{Q}$ ...

Definition. A number $n \in \mathbb{N}$ is called a *congruent number* if it is the area of a triangle whose side-lengths are all rational i.e. if $\exists a, b, c \in \mathbb{Q}$ such that $a^2 + b^2 = c^2$ and $2n = ab$.

We will soon see that congruent numbers are related to specific type of elliptic curves over $\mathbb{Q}$. But before doing that let us make some notable remarks on congruent numbers

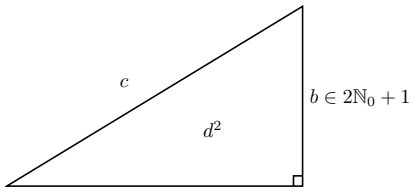
Remark 1.

• A number $n \in \mathbb{N}$ is congruent iff its square-free factor is congruent. In particular, it suffices for us to study congruent square-free numbers.

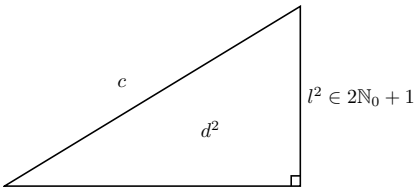
• A congruent number $n \in \mathbb{N}$ is clearly related to Pythogoras triples i.e. $(a, b, c) \in \mathbb{N}^3$ such that $a^2 + b^2 = c^2$.

The question whether a natural number is congruent has been asked since ancient times, according to Dickson this problem dates back as old as the 10th-century A.D. In the 17-th century Fermat proved that 1 cannot be a congruent number. We give a geometric illustration of the proof. Fermat popularized the so-called *(infinite) descent method*. The method takes advantage of the fact that natural numbers are bound below by 1 and is a proof by contradiction. It is assumed that a (Diophantine) solution of natural numbers exists and from this solution one obtains a solutions with even smaller natural numbers and by induction one obtains solutions with strictly decreasing numbers ad infinitum, and this we know is impossible.

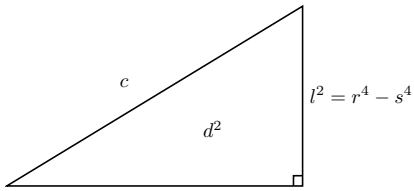
Proof of '1 is not congruent'. We give a rough illustrative proof that 1 is not a congruent number



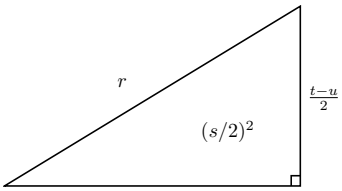
(a) $a^2 + b^2 = c^2$ and $(a, b) = 1$



(b) $4k^4 + b^2 = c^2$ and $\frac{c+b}{2}\frac{c-b}{2} = k^4$



(c) $\left(\frac{c+b}{2}, \frac{c-b}{2}\right) = 1$, so we may write $r^4 := \frac{c+b}{2}$ and $s^4 := \frac{c-b}{2}$



(d) Because $(r^2 + s^2, r^2 - s^2) = 1$, we can write $t^2 := r^2 + s^2$ and $u^2 := r^2 - s^2$ with both $t^2, u^2 \equiv 1 \bmod 4$. So $s \in 2\mathbb{N}$ and $(t, u) = 1$

Because $0 < r \leq r^4 < r^4 + s^4 = c$ and by infinite descent we get a contradiction

First we assume, by contradiction, that $\frac{a}{d} + \frac{b}{d} = \frac{c}{d}$ and without loss of generality $\gcd(a, b) = 1$. One proves then that a and b have opposite parity (i.e. one is odd and the other even) without loss of generality $a \in 2\mathbb{N}$ and we have Figure (a). But $ab = 2d^2$ with $(a, b) = 1$ so one can find $k, l \in \mathbb{N}$ with $a = 2k^2$ and $b = l^2$ and (we can show that $\left(\frac{c-b}{2}, \frac{c+b}{2}\right) = 1$) we have the equations described in (b) for some $k \in \mathbb{N}$. By the coprimality of $\frac{c-b}{2}$ and $\frac{c+b}{2}$, we realize that both must be a fourth power and so we have the equations in (c). Equations in (d) follows almost immediately, now t^2 and u^2 are odd square (they are odd because $t^2 s^2 = l^2$ is odd) and so equivalent to 1 mod 4. So $2s^2 \equiv 0 \bmod 4$ and this implies that s is even. By $r < c$ we have created a new right triangle with an area that is a square number and two adjacent sidelengths that are coprime (and thus we have created a new triangle with rational sides and area that is 1) and the contradiction follows by infinite descent. □

There is a relation between the problem of congruent numbers and elliptic curves over $\mathbb{Q}$. We can see this by first working out the following exercise

Exercise 1. Let $n \in \mathbb{N}$ and consider the elliptic curve $E_n : y^2 = x^3 - n^2 x$ over $\mathbb{Q}$ and show that

$$\operatorname{Tor}(E) = \{O, (0, 0), (-n, 0), (n, 0)\}$$

Hint: From Nagell-Lutz we know that $\#\operatorname{Tor}(E) \mid \#E(\mathbb{F}_p)$ for a good reduction of E modulo a prime p. The above is true for any good reduction and you conclude this by counting $\#E(\mathbb{F}_p)$ for good reduction modulo primes $p \equiv 3 \bmod 4$.

Now we can give the relationship between a congruent number n and the elliptic curve E_n:

Proposition 2. Let $n \in \mathbb{N}$, then there is a bijection between $E_n \setminus \operatorname{Tor}(E_n)$ (defined in above exercise) and the set

$$\{(a, b, c) \in \mathbb{Q}^3 \, : \, a^2 + b^2 = c^2 \quad ab = 2n\}$$

Construction of Bijection. We just show the bijection and allow the reader to continue with the proof. The map from the set to E_n is given by

$$(a, b, c) \mapsto \left(\frac{nb}{c - a}, \frac{2n^2}{c - a}\right)$$

and its inverse is given by

$$P \mapsto \left(\frac{x_P^2 - n^2}{y_P}, \frac{2nx_P}{y_P}, \frac{x_P^2 + n^2}{y_P} \right)$$

□

So the above theorem just says that for n to be a congruent number E_n should have a non-torsion point i.e.

Corollary 3. A number $n \in \mathbb{N}$ is a congruent number iff E_n has a positive rank.

Since we already argued that it suffices to study square-free congruent number we give a similar version to the above proposition

Theorem 4. Let $n \in \mathbb{N}$ be square-free then there is a bijection between Pythagoras triples $a, b, c \in \mathbb{Q}$ (i.e. they are the side-lengths of a right-triangle) such that $a < b < c$ with area n (i.e. $2ab = n$) and triples of square rationals $x - n, x, x + n \in \mathbb{Q}$

The rank of elliptic curves over $\mathbb{Q}$ is however one of the big mysteries in modern number theory. There are a few conjectures in mathematics related to the rank of elliptic curves over $\mathbb{Q}$, here are a few:

Some Rank Problems. The following are some unsolved problems to date

- (rank conjecture) Given a number $n \in \mathbb{N}$, there is a number $r \geq n$ and an elliptic curve $E/\mathbb{Q}$ such that the rank of E is r.
- (number of ranks 1 and 0) Assuming we can enumerate elliptic curves over $\mathbb{Q}$ up to certain bounds (e.g. by using some sort of height functions on the coefficients of its defining equations) and if E is an elliptic curve over $\mathbb{Q}$ let r_E be its rank then

$$\lim_{N \to \infty} \frac{\#\{E/\mathbb{Q} \text{ 'up to' } N, r_E = 0\}}{\#\{E/\mathbb{Q} \text{ 'up to' } N\}} = \lim_{N \to \infty} \frac{\#\{E/\mathbb{Q} \text{ 'up to' } N, r_E = 1\}}{\#\{E/\mathbb{Q} \text{ 'up to' } N\}} = 1/2$$

Let us give some remarks on the above problems

- Because of the rank conjecture, there is a race for mathematicians to find elliptic curves of high rank. The highest elliptic curve (over $\mathbb{Q}$) rank known to us is an elliptic curve of rank at least 28 by Noam Elkies. His curve has rank exactly 28 if the extended Riemann hypothesis is assumed, but otherwise he has shown that there are 28 independent non-torsion points in his elliptic curve.
- It is indeed widely believed that most elliptic curves have rank 0 and 1. At least experiments have shown us that this is highly likely. The latest development are the work of Bhargava, Skinner, Zhang, Shankar et al. who showed us that at least 83% of all elliptic curves over $\mathbb{Q}$ are rank 0 or 1.

But if a conjecture in mathematics is solved we may be able to develop some algorithms in finding ranks of elliptic curves over $\mathbb{Q}$. These conjectures are attributed to Birch and Swinnerton-Dyer ...

BSD Conjecture (old version). Let E be an elliptic curve over $\mathbb{Q}$ and suppose $r \in \mathbb{N}_0$ is its rank. Define for a prime $p \in \mathbb{N}$ the number of points in the reduction of E mod p (reduction need not be good). Then we have the following approximation as $n \to \infty$

$$\prod_{p \leq n} \frac{N_p}{p} \sim c(\log n)^r$$

for some positive constant $c \in \mathbb{R}$ (where the product runs over prime numbers p less than n).

If the above conjecture is true and if we notice that the above product does not increase as n increases (for sufficiently large n) then we can conclude that the rank of E is 0. Specifically, if $E = E_n$, then we can conclude in this case that n is not a congruent number. Tunnel has shown an easier way to check for congruent numbers if we assume BSD is true

Tunnel's Theorem. For $n \in \mathbb{N}$ define

$$A_n := \#\left\{(x,y,z) \in \mathbb{Z}^3 \ : \ \begin{array}{ll} 2x^2+y^2+32z^2=n & n \text{ odd} \\ 8x^2+2y^2+64z^2=n & n \text{ even} \end{array}\right\}$$

and

$$B_n := \#\left\{(x,y,z) \in \mathbb{Z}^3 \ : \ \begin{array}{ll} 2x^2+y^2+8z^2=n & n \text{ odd} \\ 8x^2+2y^2+16z^2=n & n \text{ even} \end{array}\right\}$$

Then if n is a congruent number one has $2A_n = B_n$. Furthermore, if BSD is true then $2A_n = B_n$ implies that n is a congruent number.

The modern version of BSD is stated using the L-function associated to an elliptic curve $E/\mathbb{Q}$

Theorem 5. Let E be an elliptic curve over $\mathbb{Q}$ and let Δ be its discriminant, define for any prime number p

$$a_p := p + 1 - \#E(\mathbb{F}_p)$$

where $E(\mathbb{F}_p)$ is the reduction of E mod p (bad reduction allowed), then the function

$$L(s) := \prod_{p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

converges and is analytic at all points $s \in \mathbb{C}$ for which $Re(s) > 3/2$ and it can be continued analytically to the whole of the complex plane.

The above function is called the L-function of E and if we naively substitute $s = 1$ for L we see that the partial product of the above is just the reciprocal of the product $\prod \frac{N_p}{p}$ in the old version of BSD. It was hypothesized that r in the old version is in fact the order of zero of the L-function at $s = 1$. This order of zero of the L-function is called the *analytic rank* i.e.

$$L(s) = c(s-1)^r + \text{ higher order terms}$$

where c is some non-zero constant.

Now we have two concept of ranks for an elliptic curve $E/\mathbb{Q}$ and we can formulate the modern version of BSD

BSD Conjecture (modern version). For an elliptic curve E over $\mathbb{Q}$ with rank r we have

$$\text{ord}_{s=1} L(s) = r$$

i.e. the analytic rank and the (algebraic) rank coincide.

There is a reward of $1M from the Clay institute if one solves the BSD conjecture!