Explicit Methods for Solving Diophantine Equations

Henri Cohen

Laboratoire A2X

Université Bordeaux 1

Tucson, Arizona Winter School, 2006

EXAMPLES (I)

Diophantine equation: system of polynomial equations to be solved in integers, rational numbers, or other number rings.

● **Fermat's Last Theorem (FLT)**: in $\mathbb{Z}$, $x^n + y^n = z^n$ with $n \geq 3$ implies $xyz = 0$. This gave the impetus for algebraic number theory by Kummer, Dirichlet, ... Solved by these methods up to large values of n (several million). Then Faltings's result on rational points on higher genus curves proved that for fixed n, only finite number of (coprime) solutions. But finally completely solved using elliptic curves, modular forms, and Galois representations by Ribet, Wiles, and Taylor–Wiles. The method of solution is more important than FLT itself.

EXAMPLES (II)

- **Catalan's conjecture**: if m and n are at least 2, nonzero solutions of $x^m - y^n = 1$ come from $3^2 - 2^3 = 1$. Until recently, same status as FLT: attacks using algebraic number theory solved many cases. Then Baker-type methods were used by Tijdeman to show that the total number of (m, n, x, y) is finite. Finally completely solved by Mihăilescu in 2001, using **only** the theory of cyclotomic fields, but rather deep results (Thaine's theorem), quite a surprise. Proof later simplified by Bilu and Lenstra.

EXAMPLES (III)

- **The congruent number problem** (Diophantus, 4th century A.D.). Find all integers n equal to the area of a Pythagorean triangle, i.e. with all sides rational (example $(3, 4, 5)$ gives $n = 6$). Easy: equivalent to the existence of rational solutions of $y^2 = x^3 - n^2x$ with $y \neq 0$. Again, three stages. Until the 1970's, several hundred values solved. Then using the Birch–Swinnerton Dyer conjecture (BSD), possible to determine conjecturally but analytically if n congruent or not. Final (but not ultimate) step: a theorem of Tunnell in 1980 giving an immediate criterion for congruent numbers, using modular forms of half-integral weight, but still modulo a weak form of BSD.

TOOLS (I)

Almost as many methods to solve Diophantine equations as equations. Attempt at classification:

● **Local methods:** the use of p-adic fields, in an elementary way (congruences modulo powers of p), or less elementary (Strassmann's or Weierstrass's theorem, p-adic power series, Herbrand's and Skolem's method).

● **Factorization over** $\mathbb{Z}$. Not a very powerful method, but sometimes gives spectacular results (Wendt's criterion for the first case of Fermat's last theorem, Cassels's results on Catalan's equation).

TOOLS (II)

● **Factorization over number fields**, i.e., global methods. This was in fact the *motivation* for the introduction of number fields in order to attack Fermat's last theorem (FLT). Even though very classical, still one of the most powerful methods, with numerous applications and successes.

● **Diophantine approximation methods.** This can come in many different guises, from the simplest such as Runge's method, to much more sophisticated ones such as Baker-type methods.

● **Modular methods,** based on the work of Ribet, Wiles, and Taylor–Wiles, whose first and foremost success is the complete solution of FLT, but which has had many applications to other problems.

Tools (III)

In addition, if the set of solutions has a well-understood structure, in many cases one can construct algorithmically this set of solutions, and in particular one solution. Examples are:

- **The Pell–Fermat equation** $x^2 - Dy^2 = \pm 1$, and more generally norm equations $\mathcal{N}_{K/\mathbb{Q}}(\alpha) = m$, where the magical algorithm is based on continued fractions and Shanks's infrastructure.

- **Elliptic curves of rank** 1 over $\mathbb{Q}$, where the magical algorithm is based on the construction of Heegner points, and in particular of the theory of complex multiplication.

Introduction to Local Methods (I)

Examples of naive use:

- **The equation $x^2 + y^2 = 3z^2$.** Dividing by the square of the GCD, we may assume x and y coprime. Then x^2 and y^2 are congruent to 0 or 1 modulo 3, but not both 0, hence $x^2 + y^2 \equiv 1 \pmod{3}$, a contradiction.

- **FLT I for exponent 3**. This is the equation $x^3 + y^3 = z^3$ with $3 \nmid xyz$. We work modulo 3^2: since a cube is congruent to 0 or ± 1 modulo 9, if $3 \nmid xy$ we have $x^3 + y^3 \equiv -2$, 0, or 2 modulo 9, which is impossible if $3 \nmid z$.

INTRODUCTION TO LOCAL METHODS (II)

In general need properties of the field $\mathbb{Q}_p$ of p-adic numbers and ring of integers $\mathbb{Z}_p$. Reminder:

• A homogeneous equation with integer coefficients has a nontrivial solution modulo p^n for all $n \geq 0$ if and only if it has a nontrivial solution in $\mathbb{Z}_p$ (or in $\mathbb{Q}_p$ by homogeneity).

• There is a canonical integer-valued valuation v_p on $\mathbb{Q}_p^*$: if $x \in \mathbb{Q}$ then $v_p(x)$ is the unique integer such that $x/p^{v_p(x)}$ can be written as a rational number with denominator and numerator not divisible by p. It is ultrametric: $v_p(x+y) \geq \min(v_p(x), v_p(y))$.

• Elements of $\mathbb{Q}_p$ such that $v_p(x) \geq 0$ are p-adic integers, they form a local ring $\mathbb{Z}_p$ with maximal ideal $p\mathbb{Z}_p$. Invertible elements of $\mathbb{Z}_p$, called p-adic units, are x such that $v_p(x) = 0$. If $x \in \mathbb{Q}_p^*$, canonical decomposition $x = p^{v_p(x)}y$ with y a p-adic unit.

Introduction to Local Methods (III)

● If $a \in \mathbb{Q}$ is such that $v_p(a) \geq 0$ and if $v_p(x) \geq 1$ then the power series $(1+x)^a$ converges. If $v_p(a) < 0$ the power series converges for $v_p(x) \geq |v_p(a)| + 1$ when $p \geq 3$, and $v_p(x) \geq |v_p(a)| + 2$ when $p = 2$. It converges to its "expected" value, for instance if $m \in \mathbb{Z} \setminus \{0\}$ then $y = (1+x)^{1/m}$ satisfies $y^m = 1 + x$.

● Hensel's lemma (or Newton's method). Special case: if $f(X) \in \mathbb{Q}_p[X]$ and $\alpha \in \mathbb{Q}_p$ satisfies $v_p(f(\alpha)) \geq 1$ and $v_p(f'(\alpha)) = 0$. There exists $\alpha^* \in \mathbb{Q}_p$ such that $f(\alpha^*) = 0$ and $v_p(\alpha^* - \alpha) \geq 1$, and α^* easily computed by Newton's iteration.

Testing for local solubility is usually easy and algorithmic.

Local Methods: The Fermat Quartics (I)

These are the equations

$$x^4 + y^4 = cz^4 \ ,$$

where without loss of generality we may assume that $c \in \mathbb{Z}$ is not divisible by a fourth power. Denote by $\mathcal{C}$ the projective curve $x^4 + y^4 = c$.

Note that we will only give the local solubility results, but that the global study involves many methods (factorization in number fields, elliptic curves), but is far from complete, although it can solve $c \leq 10000$.

LOCAL METHODS: THE FERMAT QUARTICS (II)

Proposition. *The curve $\mathcal{C}_c$ is everywhere locally soluble (i.e., has points in $\mathbb{R}$ and in every $\mathbb{Q}_p$) if and only if $c > 0$ and the following conditions are satisfied.*

1. $c \equiv 1$ *or* 2 *modulo* 16.
2. $p \mid c$, $p \neq 2$ *implies* $p \equiv 1 \pmod{8}$.
3. $c \not\equiv 3$ *or* 4 *modulo* 5.
4. $c \not\equiv 7$, 8, *or* 11 *modulo* 13.
5. $c \not\equiv 4$, 5, 6, 9, 13, 22, *or* 28 *modulo* 29.

Local Methods: The Fermat Quartics (III)

Ingredients in proof:

- A 2-adic unit x is a fourth power in $\mathbb{Q}_2$ if and only if $x \equiv 1 \pmod{16\mathbb{Z}_2}$ (power series expansion $(1+u)^{1/4}$).

- If $p \nmid 2c$ and $p \not\equiv 1 \pmod{8}$ then c is a sum of two fourth powers in $\mathbb{Q}_p$ if and only if $\overline{c}$ is a sum of two fourth powers in $\mathbb{F}_p$ (Hensel's lemma), and any such $\overline{c}$ is such a sum if $p \equiv 3 \pmod{4}$ (pigeonhole principle).

- If $p \nmid 2c$ and $p \geq 37$ then $\overline{c}$ is a sum of two fourth powers (the Weil bounds, here easily provable using Jacobi sums).

LOCAL METHODS: FERMAT'S LAST THEOREM I (I)

Proposition. *The following three conditions are equivalent.*

1. *There exists three p-adic units α, β, and γ such that $\alpha^p + \beta^p = \gamma^p$ (in other words FLT I is soluble p-adically).*
2. *There exists three integers a, b, c in $\mathbb{Z}$ such that $p \nmid abc$ with $a^p + b^p \equiv c^p \pmod{p^2}$.*
3. *There exists $a \in \mathbb{Z}$ such that a is not congruent to 0 or -1 modulo p with $(a+1)^p \equiv a^p + 1 \pmod{p^2}$.*

Proof: Congruences modulo p^3 and Hensel's lemma.

LOCAL METHODS: FERMAT'S LAST THEOREM I (II)

Corollary. *If for all* $a \in \mathbb{Z}$ *such that* $1 \leq a \leq (p-1)/2$ *we have* $(a+1)^p - a^p - 1 \not\equiv 0 \pmod{p^2}$, *the first case of FLT is true for* p.

Note that using Eisenstein reciprocity (which is a more difficult global statement), can prove that $a = 1$ is sufficient in the above, i.e., Wieferich's criterion: if $2^{p-1} \not\equiv 1 \pmod{p^2}$ then FLT I is true for p (only known exceptions $p = 1093$ and $p = 3511$).

LOCAL METHODS: STRASSMANN'S THEOREM (I)

More sophisticated use of p-adic numbers: p-adic analysis.

Theorem. *If* $f(X) = \sum_{n\ge 0} f_n X^n$ *with* $f_n \to 0$ p*-adically, not identically* 0*, exist at most* N *elements* $x \in \mathbb{Z}_p$ *such that* $f(x) = 0$*, where* N *unique integer such that* $|f_n| \le |f_N|$ *for* $n < N$*, and* $|f_n| < |f_N|$ *for* $n > N$.

Same theorem in extensions of $\mathbb{Q}_p$. Easy proof by induction on N using the ultrametric inequality.

Local Methods: Strassmann's Theorem (II)

Example: the equation $x^3 + 6y^3 = 1$ in $\mathbb{Z}$. Set $\theta = 6^{1/3}$, $K = \mathbb{Q}(\theta)$, $\varepsilon = 3\theta^2 - 6\theta + 1$ fundamental unit of K of norm 1. Dirichlet's unit theorem implies $x + y\theta = \varepsilon^k$ for $k \in \mathbb{Z}$. If $\alpha = \theta^2 - 2\theta$ then $\varepsilon = 1 + 3\alpha$, and

$$(1 + 3\alpha)^k = \exp_3(k \log_3(1 + 3\alpha))$$

power series in k (not in α) which converges 3-adically. Note 1, θ, θ^2 linearly independent over $\mathbb{Q}_3$ ($X^3 + 6$ irreducible in $\mathbb{Q}_3[X]$). Coefficient of θ^2 in $\varepsilon^k = x + y\theta + 0\theta^2$ equal to 0 gives equation in k to which can apply Strassmann, find $N = 1$, hence $k = 0$ only solution, so $(x, y) = (1, 0)$.

FACTORIZATION OVER $\mathbb{Z}$: WENDT'S CRITERION (I)

Can give spectacular results. Example: Wendt's criterion for **FLT I**.

Proposition. *Let p be an odd prime, $k \geq 2$ an even integer. Assume that $q = kp + 1$ is a prime such that $q \nmid (k^k - 1)R(X^k - 1, (X+1)^k - 1)$ ($R(P, Q)$ resultant of P and Q). Then FLT I is true, i.e., $x^p + y^p + z^p = 0$ implies $p \mid xyz$.*

Proof: May assume relatively prime. Write

$$-x^p = y^p + z^p = (y+z)(y^{p-1} - y^{p-2}z + \cdots + z^{p-1})\ .$$

Observe factors relatively prime (otherwise y and z not relatively prime). Thus exists a such that $y + z = a^p$ and $y^{p-1} - y^{p-2}z + \cdots + z^{p-1} = s^p$. By symmetry $z + x = b^p$ and $x + y = c^p$.

FACTORIZATION OVER $\mathbb{Z}$: WENDT'S CRITERION (II)

For $q = kp + 1$, equation implies

$$x^{(q-1)/k} + y^{(q-1)/k} + z^{(q-1)/k} \equiv 0 \pmod{q} .$$

If $q \nmid xyz$, implies that $u = (x/z)^p \bmod q$ satisfies $u^k - 1 \equiv 0 \pmod{q}$ and $(u+1)^k \equiv 0 \pmod{q}$, contradicting $q \nmid R(X^k - 1, (X+1)^k - 1)$. Thus $q \mid xyz$, say $q \mid x$, hence

$$\begin{aligned} 0 \equiv 2x = (x+y) + (z+x) - (y+z) &= c^p + b^p + (-a)^p \\ &= c^{(q-1)/k} + b^{(q-1)/k} + (-a)^{(q-1)/k} \pmod{q} . \end{aligned}$$

As above, $q \mid abc$, and since $q \mid x$ and x, y, and z pairwise coprime, cannot have $q \mid b^p = z + x$ or $q \mid c^p = x + y$, so $q \mid a$.

FACTORIZATION OVER $\mathbb{Z}$: WENDT'S CRITERION (III)

Thus $y \equiv -z \pmod{q}$, hence $s^p \equiv py^{p-1} \pmod{q}$. On the other hand $y = (x+y) - x \equiv c^p \pmod{q}$, so

$$s^{(q-1)/k} = s^p \equiv pc^{((q-1)/k)(p-1)} \pmod{q} ,$$

and since $q \nmid c$, $p \equiv d^{(q-1)/k} \pmod{q}$ with $d = s/c^{p-1} \bmod q$. Since a, s coprime, we have $q \nmid s$, so $q \nmid d$, so $p^k \equiv 1 \pmod{q}$, and since k even

$$1 = (-1)^k = (kp - q)^k \equiv k^k p^k \equiv k^k \pmod{q} ,$$

contradicting the assumption $q \nmid k^k - 1$.

FACTORIZATION OVER $\mathbb{Z}$: WENDT'S CRITERION (IV)

Wendt's criterion (of course superseded by Wiles et al.) is very powerful since heuristically there will **always** exist a suitable k, in fact quite small, and computer searches confirm this.

Corollary due to Sophie Germain:

Corollary. *If* $p > 2$ *is prime and* $2p + 1$ *is prime then FLT I is true.*

Unknown whether there are infinitely many.

FACTORIZATION OVER $\mathbb{Z}$: $y^2 = x^3 + t$

By using similar naive methods, can prove the following:

● If a and b are odd, if $3 \nmid b$, and if $t = 8a^3 - b^2$ is squarefree, then $y^2 = x^3 + t$ has no **integral** solution.

The example $t = 7 = 8 \cdot 1^3 - 1^2$ was a challenge posed by Fermat.

● If a is odd, $3 \nmid b$, and $t = a^3 - 4b^2$ is squarefree and such that $t \not\equiv 1 \pmod 8$. Then $y^2 = x^3 + t$ has no **integral** solution.

Cassels's results on Catalan (I)

Recall that Catalan's equation is $x^m - y^n = 1$, with $\min(m,n) \geq 2$. Contrary to FLT, $m = 2$ or $n = 2$ must be included. Proof for $n = 2$ (no nontrivial solution) due to V.-A. Lebesgue in 1850 (not the Lebesgue integral), and involves factoring over $\mathbb{Z}[i]$, not difficult. Proof for $m = 2$ considerably more subtle (not really difficult) because there **exist** the solutions $(\pm 3)^2 - 2^3 = 1$. Done by Ko Chao in the 1960's, and involves structure of the unit group of a real quadratic **order**.

As for FLT, we are reduced to $x^p - y^q = 1$ with p and q distinct odd primes, with symmetry map $(p, q, x, y) \mapsto (q, p, -y, -x)$. Basic results on this found by Cassels.

CASSELS'S RESULTS ON CATALAN (II)

Cassels's proof: factoring over $\mathbb{Z}$, clever reasoning, and analytic method called Runge's method, a form of Diophantine approximation. As all such, boils down to $x \in \mathbb{R}$, $|x| < 1$, and $x \in \mathbb{Z}$ implies $x = 0$.

Exercise: use this to find all integral solutions to $y^2 = x^4 + x^3 + x^2 + x + 1$ (hint in the notes).

Need arithmetic lemma and two analytic ones.

- **Arithmetic lemma**: Let q prime, and set $w(j) = j + v_q(j!)$. Then $q^{w(j)}\binom{p/q}{j}$ is an **integer coprime to** q, and $w(j)$ is **strictly increasing**.

Proof: easy, although there is a slight subtlety (see notes).

Cassels's results on Catalan (III)

- **Analytic lemma I**: If $q > p > 0$ (not necessarily integral) and $a \geq 1$, then $(a^q + 1)^p < (a^p + 1)^q$, and if $a > 1$ then $(a^q - 1)^p > (a^p - 1)^q$.

Proof: easy undergraduate exercise.

- **Analytic lemma II**: Assume $p > q$ integers, $q \geq 3$, $p \geq 5$ as in Catalan. Set $F(t) = ((1+t)^p - t^p)^{1/q}$, $m = \lfloor p/q \rfloor + 1$, and let $F_m(t)$ the sum of the terms of degree at most equal to m in the Taylor series expansion of $F(t)$ around $t = 0$. For all $t \in \mathbb{R}$ such that $|t| \leq 1/2$ we have

$$|F(t) - F_m(t)| \leq \frac{|t|^{m+1}}{(1-|t|)^2} \ .$$

Proof: not easy undergraduate exercise (see notes).

CASSELS'S RESULTS ON CATALAN (IV)

Factorization over $\mathbb{Z}$: $x^p - y^q = 1$ gives $y^q = x^p - 1 = (x-1)r_p(x)$ with $r_p(x) = (x^p - 1)/(x-1)$. Factors not necessarily coprime but, expanding $r_p(x) = ((x-1+1)^p - 1)/(x-1)$ by the binomial theorem, easy to see that $p \mid (x-1)$ is equivalent to $p \mid r_p(x)$, that if $d = \gcd(x-1, r_p(x))$ then $d = 1$ or $d = p$, and that if $d = p > 2$ then $r_p(x) \equiv p \pmod{p^2}$, so that $v_p(r_p(x)) = 1$. Since $y^q = (x-1)r_p(x)$, condition $d = p$ is equivalent to $p \mid y$. Cassels's main theorem says that this is **always** true, i.e., we never have $d = 1$.

CASSELS'S RESULTS ON CATALAN (V)

Proof of Cassels's result split into $p < q$ and $p > q$. The first case is much easier:

Proposition. *If x and y are nonzero integers and p and q odd primes such that $x^p - y^q = 1$, then when $p < q$ we have $p \mid y$.*

Proof: if not, $x - 1$ and $r_p(x)$ are coprime, so both are qth powers since product is. Write $x - 1 = a^q$. Since $xy \neq 0$, $a \neq 0$ and $a \neq -1$, and $(a^q + 1)^p - y^q = 1$. Set $f(z) = (a^q + 1)^p - z^q - 1$, decreasing function of z. If $a \geq 1$ then $f(a^p) = (a^q + 1)^p - a^{pq} - 1 > 0$ (binomial theorem), and $f(a^p + 1) = (a^q + 1)^p - (a^p + 1)^q - 1 < 0$ by first analytic lemma. Since f strictly decreasing, the y such that $f(y) = 0$ is not an integer, absurd.

Cassels's results on Catalan (VI)

Similarly, if $a < 0$, we have $a \leq -2$, and set $b = -a$. Since p and q are odd $f(a^p) = (a^q+1)^p - a^{pq} - 1 = -((b^q-1)^p - b^{pq} + 1) > 0$ (binomial theorem), and $f(a^p+1) = (a^q+1)^p - (a^p+1)^q - 1 = -((b^q-1)^p - (b^p-1)^q + 1) < 0$ again by the first analytic lemma since $b > 1$. Again absurd.

Crucial corollary, due to Hyyrö:

Corollary. *Same assumptions, in particular $p < q$. Then $|y| \geq p^{q-1} + p$.*

Proof: since $p \mid y$ and $v_p(r_p(x)) = 1$, can write $x - 1 = p^{q-1}a^p$, $(x^p-1)/(x-1) = pv^q$, $y = pav$. Set $P(X) = X^p - 1 - p(X-1)$. Clearly $(X-1)^2 \mid P(X)$, so $(x-1) \mid (x^p-1)/(x-1) - p = p(v^q-1)$, so $v^q \equiv 1 \pmod{p^{q-2}}$. Since $q > p$, $\phi(p^{q-2}) = p^{q-3}(p-1)$ coprime to q, hence $v \equiv 1 \pmod{p^{q-2}}$. It is easily seen that $v = 1$ is impossible, so $v \geq p^{q-2} + 1$, so $|y| = pav \geq pv \geq p^{q-1} + p$.

Cassels's results on Catalan (VII)

Case $p > q$ more difficult.

Proposition. *If x and y are nonzero integers and p and q odd primes such that $x^p - y^q = 1$, then when $p > q$ we have $p \mid y$.*

Proof: as in proof for $p < q$, assume by contradiction $p \nmid y$, so $x - 1 = a^q$ hence $y^q = (a^q + 1)^p - 1$, so $y = a^p F(1/a^q)$ with F as in analytic lemma II. Recall $m = \lfloor p/q \rfloor + 1$, and set $z = a^{mq-p}y - a^{mq}F_m(1/a^q)$, so that $z = a^{mq}(F(1/a^q) - F_m(1/a^q))$. By Taylor's theorem $t^m F_m(1/t) = \sum_{0 \le j \le m} \binom{p/q}{j} t^{m-j}$, and by arithmetic lemma $D = q^{m+v_q(m!)}$ is a common denominator of all the $\binom{p/q}{j}$ for $0 \le j \le m$. Thus $Da^{mq}F_m(1/a^q) \in \mathbb{Z}$, and since $mq \ge p$ we have $a^{mq-p}y \in \mathbb{Z}$, so that $Dz \in \mathbb{Z}$.

CASSELS'S RESULTS ON CATALAN (VIII)

We now show $|Dz| < 1$. Applying analytic lemma II to $t = 1/a^q$ (satisfies $|t| \leq 1/2$ since $a \neq \pm 1$):

$$|z| \leq \frac{|a|^q}{(|a|^q - 1)^2} \leq \frac{1}{|a|^q - 2} \leq \frac{1}{|x| - 3} \; .$$

By Hyyrö's Corollary (with (p, q, x, y) replaced by $(q, p, -y, -x)$) we have $|x| \geq q^{p-1} + q \geq q^{p-1} + 3$, so

$$|Dz| \leq \frac{D}{|x| - 3} \leq q^{m + v_q(m!) - (p-1)} \; .$$

Since $v_q(m!) < m/(q-1)$ for $m \geq 1$ and $m < p/q + 1$, we have

$$m + v_q(m!) - (p-1) < m\frac{q}{q-1} - (p-1) = \frac{3 - (p-2)(q-2)}{q-1} \leq 0$$

since $q \geq 3$ and $p \geq 5$, proving $|Dz| < 1$.

Cassels's results on Catalan (IX)

Since $Dz \in \mathbb{Z}$, we have $Dz = 0$. But

$$Dz = Da^{mq-p}y - \sum_{0 \le j \le m} D\binom{p/q}{j} a^{q(m-j)} ,$$

and by the arithmetic lemma

$$v_q\left(\binom{p/q}{j}\right) < v_q\left(\binom{p/q}{m}\right) = v_q(D)$$

for $0 \le j \le m-1$, hence again by the arithmetic lemma

$$0 = Dz \equiv D\binom{p/q}{m} \not\equiv 0 \pmod{q} ,$$

absurd.

Cassels's results on Catalan (IX)

Immediate but crucial corollary of Cassels's theorem:

Corollary. *If x and y are nonzero integers and p and q odd primes such that $x^p - y^q = 1$, there exist nonzero integers a and b, and positive integers u and v with $q \nmid u$ and $p \nmid v$ such that*

$$x = qbu,\ x - 1 = p^{q-1}a^q,\ \frac{x^p - 1}{x - 1} = pv^q,$$
$$y = pav,\ y + 1 = q^{p-1}b^p,\ \frac{y^q + 1}{y + 1} = qu^p\ .$$

Proof: easy exercise from the main theorem.

Introduction to Number Fields (I)

Apart from the methods studied above, this is the oldest and most used method in the subject, and as already mentioned the whole theory of number fields arose from the study of Diophantine equations, in particular FLT. Reminder:

● A **number field** K is a finite extension of $\mathbb{Q}$, equivalently $K = \mathbb{Q}(\alpha)$, where α root of a nonzero polynomial $A \in \mathbb{Q}[X]$.

● An **algebraic integer** is a root of a **monic** polynomial with integer coefficients. The element α such that $K = \mathbb{Q}(\alpha)$ can always be chosen such. The set of algebraic integers of K forms a ring, denoted $\mathbb{Z}_K$, containing $\mathbb{Z}[\alpha]$ with finite index, when α chosen integral. It is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$, and a $\mathbb{Z}$-basis of $\mathbb{Z}_K$ is called an **integral basis**.

Introduction to Number Fields (II)

● The ring $\mathbb{Z}_K$ is a **Dedekind domain**. The essential consequence is that any fractional ideal can be decomposed uniquely into a power product of prime ideals. This is in fact the main motivation. Crucial fact: if $\mathbb{Z}[\alpha] \neq \mathbb{Z}_K$ then it is **never** a Dedekind domain.

● If p is a prime, let $p\mathbb{Z}_K = \prod_{1 \le i \le g} \mathfrak{p}_i^{e_i}$ be the prime power decomposition of $p\mathbb{Z}_K$. The ideals $\mathfrak{p}_i$ are the prime ideals "above" (in other words containing) p, the e_i are the ramification indexes, the field $\mathbb{Z}_K/\mathfrak{p}_i$ is a finite field containing $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with degree denoted by f_i, and we have the important relation $\sum_{1 \le i \le g} e_i f_i = n = [K : \mathbb{Q}]$.

INTRODUCTION TO NUMBER FIELDS (III)

- **Class group** $Cl(K)$ defined as the quotient of fractional ideals by principal ideals, **finite** group with cardinality denoted $h(K)$.

- **Unit group** $U(K)$, group of invertible elements of $\mathbb{Z}_K$, or group of algebraic **integers** of norm ± 1, is a **finitely generated** abelian group of rank $r_1 + r_2 - 1$ (r_1 and $2r_2$ number of real and complex embeddings). Torsion subgroup finite equal to the group $\mu(K)$ of roots of unity in K.

Introduction to Number Fields (IV)

- A **quadratic field** is $\mathbb{Q}(\sqrt{t})$, with t squarefree integer different from 1. Its ring of integers is either equal to $\mathbb{Z}[\sqrt{t}] = \{a + b\sqrt{t},\ a, b \in \mathbb{Z}\}$ when $t \equiv 2$ or 3 modulo 4, or $(a + b\sqrt{t})/2$, with a and b integers of same parity otherwise.

- A **cyclotomic field** is $K = \mathbb{Q}(\zeta)$, with ζ primitive mth root of unity. Main result: the ring of integers of a cyclotomic field is $\mathbb{Z}[\zeta]$, and no larger.

FERMAT'S LAST THEOREM I (FLT I) (I)

Even though Wendt's criterion is probably always applicable, it is necessary also to study the algebraic method, because it also applies to FLT II, i.e., the case $p \mid xyz$.

Notation: $\zeta = \zeta_p$ primitive pth root of 1, $K = \mathbb{Q}(\zeta)$, $\mathbb{Z}_K = \mathbb{Z}[\zeta]$, $\pi = 1 - \zeta$, $\mathfrak{p} = \pi\mathbb{Z}_K$ unique prime ideal above p, and such that $\mathfrak{p}^{p-1} = p\mathbb{Z}_K$.

At first, people thought that $\mathbb{Z}_K$ is always a unique factorization domain. Unfortunately, completely false: on the contrary, only a (known) finite list of p are such.

FERMAT'S LAST THEOREM I (FLT I) (II)

Anyway, let's assume first that $\mathbb{Z}_K = \mathbb{Z}[\zeta]$ is a UFD. We prove:

Lemma. *Assume that* $\mathbb{Z}[\zeta]$ *is a UFD. If* $x^p + y^p = z^p$ *with* $p \nmid xyz$*, there exist* $\alpha \in \mathbb{Z}[\zeta]$ *and a unit* u *of* $\mathbb{Z}[\zeta]$ *such that* $x + y\zeta = u\alpha^p$.

Proof: may assume x, y, z pairwise coprime. Our equation can be factored over $\mathbb{Z}[\zeta]$ as

$$(x+y)(x+y\zeta)\cdots(x+y\zeta^{p-1}) = z^p\ .$$

Claim: the factors are pairwise coprime. If some ω divides $x + y\zeta^i$ and $x + y\zeta^j$ for $i \neq j$, it divides also $y(\zeta^i - \zeta^j)$ and $x(\zeta^j - \zeta^i)$, hence $\zeta^i - \zeta^j$ since x and y are coprime (in $\mathbb{Z}$ hence in $\mathbb{Z}[\zeta]$). Since $(\zeta^i - \zeta^j) \mid p$ in $\mathbb{Z}[\zeta]$, we have $\omega \mid p$, and on the other hand $\omega \mid (x + y\zeta^i) \mid z$. Since p and z are coprime, $\omega \mid 1$, in other words is a unit, proving the claim.

Fermat's last theorem I (FLT I) (III)

Thus product of pairwise coprime elements in $\mathbb{Z}[\zeta]$ equal to a pth power, so up to multiplication by a unit, each one is, since $\mathbb{Z}[\zeta]$ is a PID by assumption, proving the lemma.

Unfortunately, as mentioned, not very useful since condition too strict. This is where ideals play their magic. Denote by h_p the class number of the cyclotomic field $K = \mathbb{Q}(\zeta_p)$. Then:

FERMAT'S LAST THEOREM I (FLT I) (IV)

The above lemma is still valid if we only assume $p \nmid h_p$.

To see why, note that the proof of the lemma is valid verbatim if we replace "elements" by "ideals": there is unique factorization in ideals, the coprimeness of the factors remain, and we deduce that each ideal $\mathfrak{a}_i = (x + y\zeta^i)\mathbb{Z}_K$ is a pth power of an ideal, say $\mathfrak{a}_i = \mathfrak{b}_i^p$. Crucial ingredient: since the class number is finite, $\mathfrak{b}_i^{h_p}$ is a principal ideal. Since $\mathfrak{b}_i^p$ also is, and $pu + h_p v = 1$ for some u, v, it follows that $\mathfrak{b}_i$ itself is principal. If $\mathfrak{b}_1 = \alpha\mathbb{Z}_K$ then $\mathfrak{a}_1 = (x + y\zeta)\mathbb{Z}_K = \alpha^p\mathbb{Z}_K = \mathfrak{b}_1^p$, so $x + y\zeta = u\alpha^p$ for some unit u, proving the lemma.

Fermat's last theorem I (FLT I) (V)

- The rest of the proof in case $p \nmid h_p$ is specific and easy (see notes). It uses however an additional crucial ingredient, Kronecker's theorem: if α is an algebraic **integer** such that all the conjugates of α in $\mathbb{C}$ have norm equal to 1, then it is a root of unity. In particular, if u is a unit of $\mathbb{Z}[\zeta]$, then $\overline{u}/u$ is a root of unity.

- A prime such that $p \nmid h_p$ is called a regular prime. Known that there are infinitely many **irregular** primes, conjectured infinitely many regular with density $e^{-1/2} = 0.607\ldots$.

FERMAT'S LAST THEOREM I (FLT I) (VI)

- One of the crucial ingredients in the proof was $\mathfrak{b}^{h_p}$ principal for all ideals $\mathfrak{b}$. We say that h_p annihilates the class group $Cl(K)$. However, $K/\mathbb{Q}$ is a Galois extension (even abelian) with Galois group $G \simeq (\mathbb{Z}/p\mathbb{Z})^*$. The group ring $\mathbb{Z}[G]$ acts on $Cl(K)$, and we can look for other elements of $\mathbb{Z}[G]$ which annihilate $Cl(K)$. One such is given by the Stickelberger element, and more generally elements of the Stickelberger ideal.

FERMAT'S LAST THEOREM I (FLT I) (VII)

This is used in a **simple way** by Mihăilescu for Catalan: if $x^p - y^q = 1$ with p, q odd primes and $xy \neq 0$, then double Wieferich condition:

$$p^{q-1} \equiv 1 \pmod{q^2} \quad \text{and} \quad q^{p-1} \equiv 1 \pmod{p^2} \; .$$

Note no class number condition. Only seven such pairs known, but expect infinitely many.

More sophisticated annihilator of $Cl(K)$ given by Thaine's theorem, used in an essential way by Mihăilescu for the complete proof of Catalan, but also in different contexts such as the Birch and Swinnerton-Dyer conjecture.

$y^2 = x^3 + t$ REVISITED

Have already seen in special cases. Can factor in $\mathbb{Q}(\sqrt{t})$ or in $\mathbb{Q}(\sqrt[3]{t})$. Problem with **units** which are not roots of unity. Sometimes can take care of that, but not always. $\mathbb{Q}(\sqrt[3]{t})$ always has such units, so we do not use. $\mathbb{Q}(\sqrt{t})$ also does if $t > 0$, so we assume $t < 0$. Thus write $(y - \sqrt{t})(y + \sqrt{t}) = x^3$ in **imaginary** quadratic field $K = \mathbb{Q}(\sqrt{t})$. If factors not coprime, much more messy. To have factors coprime need both t **squarefree** and $t \not\equiv 1 \pmod 8$. The first condition is not really essential, the second is. We then deduce that the ideal $(y - \sqrt{t})\mathbb{Z}_K$ is the cube of an ideal, and to conclude as in FLT I we absolutely need the condition $3 \nmid |Cl(K)|$. Under all these restrictions, easy to give complete solution (see notes). For **specific** t, must solve Thue equations.

THE SUPER-FERMAT EQUATION $x^p + y^q = z^r$ (I)

A whole course to itself! Most salient points:

• Must **add** the condition x, y, z coprime because not homogeneous, otherwise usually easy to construct infinitely many "stupid" (nontrivial) solutions. Example:

$$5526847993018333947494 4^3 + 50779978334208^5 = 6530347008^7 \; .$$

Set $\chi = 1/p + 1/q + 1/r - 1$. Different behavior according to **sign** of χ:

• If $\chi > 0$ (elliptic case) **complete and disjoint parametrizations** of the (infinite) set of solutions (Beukers).

• If $\chi < 0$, only a **finite** number of solutions (Darmon–Granville, using Faltings). Only a few cases solved (rational points on curves of genus $g \geq 1$), and only ten cases known. Would need **effective form** of Faltings.

THE SUPER-FERMAT EQUATION $x^p + y^q = z^r$ (II)

Elliptic case corresponds up to permutation to $(p, q, r) = (2, 2, r)$ (dihedral case), $(p, q, r) = (2, 3, 3)$ (tetrahedral case), $(p, q, r) = (2, 3, 4)$ (octahedral case), and $(p, q, r) = (2, 3, 5)$ (icosahedral case), because they correspond to the finite subgroups of $PSL_2(\mathbb{C})$.

Two totally different methods to treat the elliptic case. The first is again factoring over suitable number fields (never very large). The proofs are tedious and in the notes for some dihedral cases (very easy), and the octahedral case $(p, q, r) = (2, 4, 3)$. In the latter we only use $\mathbb{Z}[i]$ by writing $x^2 + y^4 = z^3$ as $(x + y^2 i)(x - y^2 i) = z^3$. One obtains exactly **four** disjoint homogeneous 2-variable parametrizations of the coprime solutions. Existence not surprising, their disjointness (i.e., any coprime solution is represented by a single parametrization) more surprising.

THE SUPER-FERMAT EQUATION $x^p + y^q = z^r$ (III)

For completeness, they are the following:

$$\begin{cases} x = 4ts(s^2 - 3t^2)(s^4 + 6t^2s^2 + 81t^4)(3s^4 + 2t^2s^2 + 3t^4) \\ y = \pm(s^2 + 3t^2)(s^4 - 18t^2s^2 + 9t^4) \\ z = (s^4 - 2t^2s^2 + 9t^4)(s^4 + 30t^2s^2 + 9t^4) \ , \end{cases}$$

with $s \not\equiv t \pmod 2$ and $3 \nmid s$.

$$\begin{cases} x = \pm(4s^4 + 3t^4)(16s^8 - 408t^4s^4 + 9t^8) \\ y = 6ts(4s^4 - 3t^4) \\ z = 16s^8 + 168t^4s^4 + 9t^8 \ , \end{cases}$$

with t odd and $3 \nmid s$.

THE SUPER-FERMAT EQUATION $x^p + y^q = z^r$ (IV)

$$\begin{cases} x = \pm(s^4 + 12t^4)(s^8 - 408t^4s^4 + 144t^8) \\ y = 6ts(s^4 - 12t^4) \\ z = s^8 + 168t^4s^4 + 144t^8 \ , \end{cases}$$

with s odd and $3 \nmid s$.

$$\begin{cases} x = \pm 2(s^4 + 2ts^3 + 6t^2s^2 + 2t^3s + t^4)(23s^8 - 16ts^7 - 172t^2s^6 - 112t^3s^5 \\ \qquad - 22t^4s^4 - 112t^5s^3 - 172t^6s^2 - 16t^7s + 23t^8) \\ y = 3(s-t)(s+t)(s^4 + 8ts^3 + 6t^2s^2 + 8t^3s + t^4) \\ z = 13s^8 + 16ts^7 + 28t^2s^6 + 112t^3s^5 + 238t^4s^4 \\ \qquad + 112t^5s^3 + 28t^6s^2 + 16t^7s + 13t^8 \ , \end{cases}$$

with $s \not\equiv t \pmod 2$ and $s \not\equiv t \pmod 3$.

THE SUPER-FERMAT EQUATION $x^p + y^q = z^r$ (V)

The factoring method works in all elliptic cases **except** in the icosahedral case $(p, q, r) = (2, 3, 5)$. Here we must use a completely different tool (applicable also in the other elliptic cases), invented in this context by F. Klein, but reinterpreted in modern terms by Grothendieck and Belyi, the theory of dessins d'enfants. This is a term coined by Grothendieck to describe coverings of $\mathbb{P}^1(\mathbb{C})$ ramified in at most 3 points. Using this, obtain in an **algorithmic manner** complex polynomials P, Q, and R (homogeneous in two variables) such that (for instance) $P^2 + Q^3 = R^5$. These polynomials can in fact be chosen with coefficients in a **number field**, and by making $PSL_2(\mathbb{C})$ act on them and introducing a suitable reduction theory, can find all parametrizations. Program initiated by F. Beukers and finished by his student J. Edwards (27 disjoint parametrizations).

INTRODUCTION TO ELLIPTIC CURVES (I)

A very important set of Diophantine equations is the search for rational points (or sometimes integral points) on curves. Curves are best classified by their genus, related to the degree. Example: a nonsingular plane curve of degree d has genus $g = (d-1)(d-2)/2$ (so $g = 0$ for lines and conics, $g = 1$ for plane cubics, $g = 3$ for plane quartics). A hyperelliptic curve $y^2 = f(x)$ where f has degree d and no multiple roots has genus $g = \lfloor (d-1)/2 \rfloor$ (so $g = 0$ for $d = 1$ or 2, $g = 1$ for $d = 3$ or 4, $g = 2$ for $d = 5$ or 6.

An elliptic curve E over some field K is a curve of genus 1, together with a K-rational point.

INTRODUCTION TO ELLIPTIC CURVES (II)

Study of elliptic curves important for many reasons: curves of genus zero very well understood (everything algorithmic). curves of genus $g \geq 2$ very difficult to handle; in addition, elliptic curves have a **very rich structure**, coming in particular from the fact that they have a natural **group law**. Reminder on elliptic curves:

- In practice, an elliptic curve can be given by equations. The simplest is as a simple Weierstrass equation $y^2 = x^3 + ax^2 + bx + c$, or a generalized Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ (canonical numbering), together with the condition that the curve be nonsingular. More generally nonsingular plane cubic with rational point, hyperelliptic quartic with square leading coefficient $y^2 = a^2x^4 + bx^3 + cx^2 + dx + e$, intersection of two quadrics, and so on. All these other realizations can algorithmically be transformed into Weierstrass form, so we will assume from now on that this is the case.

Introduction to Elliptic Curves (III)

- Set of projective points of an elliptic curve (if $y^2 = x^3 + ax^2 + bx + c$, affine points plus the point at infinity $\mathcal{O} = (0 : 1 : 0)$) form an **abelian group** under the secant and tangent method of Fermat (brief explanation: if P and Q are distinct points on the curve, draw the line joining P and Q; it meets the curve in a third point R, and $P + Q$ is the symmetrical point of R with respect to the x-axis. If $P = Q$, do the same with the tangent). **Warning**: if equation of elliptic curve is not a plane cubic, the geometric construction of the group law must be modified.

- If $K = \mathbb{C}$, $E(\mathbb{C})$ in canonical bijection with a quotient $\mathbb{C}/\Lambda$, where Λ is a **lattice** of $\mathbb{C}$, thanks to the Weierstrass $\wp$ function and its derivative.

INTRODUCTION TO ELLIPTIC CURVES (IV)

- If $K = \mathbb{F}_q$, important Hasse bound $|E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$. Essential in particular in cryptography.

- If $K = \mathbb{Q}_p$ (or a finite extension), we have a good understanding of $E(\mathbb{Q}_p)$ thanks in particular to Kodaira, Néron, and Tate.

- And what if $K = \mathbb{Q}$ (or a number field)? Most interesting, and most difficult case. Deserves a theorem to itself.

INTRODUCTION TO ELLIPTIC CURVES (V)

This is the theorem of Mordell, generalized by Weil to number fields and to Abelian varieties.

Theorem. *If E is an elliptic curve over a number field K, the group $E(K)$ is a* **finitely generated** *abelian group (the Mordell–Weil group of E over K).*

Thus $E(K) \simeq E(K)_{\text{tors}} \oplus \mathbb{Z}^r$, with $E(K)_{\text{tors}}$ a finite group, and r is called the rank of $E(K)$. $E(K)_{\text{tors}}$ is easily and algorithmically computable, and only a finite number of possibilities for it, known for instance for $K = \mathbb{Q}$ by a difficult theorem of Mazur.

One of the major unsolved problems on elliptic curves is to compute algorithmically the rank r, together with a system of generators.

Introduction to Elliptic Curves (VI)

Goal of the rest of the course: explain methods to compute $E(\mathbb{Q})$, either rigorously, or heuristically. There is no general algorithm, but only partial ones, which luckily work in "most" cases. Sample techniques:

● 2-**descent**, with or without a rational 2-torsion point

● 3-**descent** with rational torsion subgroup (more general descents possible, but for the moment not very practical, work in progress of a lot of people, some present here).

INTRODUCTION TO ELLIPTIC CURVES (VII)

- Use of L-**functions** to compute the rank, but not the generators.

- The Heegner point method, one of the most beautiful and amazing aspects of this subject, important both in theory and in practice, applicable to **rank** 1 curves, which should form the vast majority of curves of nonzero rank, the only ones where we must work. This is also the subject of the student project.

2-DESCENT WITHOUT 2-TORSION POINT (I)

The general idea of descent, initiated by Fermat, is to map a (possibly large) point on a given curve (or more general variety) to smaller points on other curves. Here smaller means that the number of digits is divided by some $k > 1$, so it is very efficient when applicable.

The simplest is 2-descent on an elliptic curve when there exists a rational 2-torsion point (see text). We study the slightly more complicated case where such a point does not exist. In other words, let $y^2 = x^3 + ax + b$, where we assume a and b in $\mathbb{Z}$ and $x^3 + ax + b = 0$ without rational roots, hence irreducible over $\mathbb{Q}$. Denote by θ a root, and set $K = \mathbb{Q}(\theta)$.

2-Descent without 2-torsion point (II)

Define the map α from $E(\mathbb{Q})$ to $K^*/{K^*}^2$ by $\alpha(\mathcal{O}) = 1$ and $\alpha((x,y)) = x - \theta$ modulo ${K^*}^2$. Fundamental result, easy to prove using definition of group law by secant and tangent:

Proposition. *α is a group homomorphism whose kernel is equal to $2E(\mathbb{Q})$. In particular, it induces an injective homomorphism from $E(\mathbb{Q})/2E(\mathbb{Q})$ to $K^*/{K^*}^2$, and the rank r of $E(\mathbb{Q})$ is equal to $\dim_{\mathbb{F}_2}(\mathrm{Im}(\alpha))$.*

(Note that we assume no 2-torsion.)

2-Descent without 2-torsion point (III)

Thus describe $\mathrm{Im}(\alpha)$. For this need T-Selmer group of a **number field** (not of the elliptic curve).

- T finite set of prime ideals of K.

- $U_T(K)$ group of T-units u of K ($v_{\mathfrak{p}}(u) = 0$ for $p \notin T$).

- $Cl_T(K)$ T-class group, equal to $Cl(K)/ < T >$ with evident notation.

- A T-virtual square $u \in K^*$ is such that $2 \mid v_{\mathfrak{p}}(u)$ for all $\mathfrak{p} \notin T$.

- The T-Selmer group $S_T(K)$ is the quotient of the group of T-virtual squares by the group ${K^*}^2$ of nonzero squares.

2-DESCENT WITHOUT 2-TORSION POINT (IV)

We have $S_T(K) \simeq (U_T(K)/U_T(K)^2) \times Cl_T(K)[2]$, so easily computable using a computer algebra system.

Basic result linking $\mathrm{Im}(\alpha)$ with $S_T(K)$ (not difficult):

Proposition. *Let T be the set of prime ideals $\mathfrak{q}$ such that $\mathfrak{q} \mid 3\theta^2 + a$ and $q \mid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$, where q prime number below $\mathfrak{q}$. Then $\mathrm{Im}(\alpha)$ is equal to the group of $\overline{u} \in S_T(K)$ such that $\mathcal{N}_{K/\mathbb{Q}}(u)$ (for any lift u) is a square in $\mathbb{Q}$ and such that there exists a lift u of the form $x - \theta$.*

- Sometimes $[\mathbb{Z}_K : \mathbb{Z}[\theta]] = 1$ so $T = \emptyset$ (but $S_T(K)$ may still be nontrivial).

- The condition on the norm is algorithmic. Unfortunately the existence of a lift u of the form $x - \theta$ is not (but luckily feasible in many cases).

2-Descent without 2-torsion point (V)

So let G the group of $\overline{u} \in S_T(K)$ whose lifts have square norm. To determine if $\overline{u}$ has a lift $x - \theta$: write $u = u_2\theta^2 + u_1\theta + u_0$ for any lift, $u_i \in \mathbb{Q}$. All lifts are of the form $u\gamma^2$ for $\gamma = c_2\theta^2 + c_1\theta + c_0$, and

$$u\gamma^2 = q_2(c_0, c_1, c_2)\theta^2 - q_1(c_0, c_1, c_2)\theta + q_0(c_0, c_1, c_2) \ ,$$

with q_i explicit quadratic forms. Condition reads $q_2(c_0, c_1, c_2) = 0$ and $q_1(c_0, c_1, c_2) = 1$. The first equation can be checked for solubility by Hasse–Minkowski (local-global principle for quadratic form), and then parametrized by quadratic forms in two variables (as super-Fermat equation). Replacing in second equation gives quartic, and dehomogenenizing gives a hyperelliptic quartic equation $y^2 = Q(x)$.

2-DESCENT WITHOUT 2-TORSION POINT (VI)

If not everywhere locally soluble, can again exclude $\overline{u}$. Otherwise search for solutions. If found, $\overline{u} \in \mathrm{Im}(\alpha)$, if not we are stuck.

The group of $\overline{u} \in S_T(K)$ for which the corresponding quartic is everywhere locally soluble is called the 2-Selmer group of the **elliptic curve**, and is the smallest group containing $E(\mathbb{Q})/2E(\mathbb{Q})$ which can be determined algorithmically using 2-descent. It is denoted $S_2(E)$. The quotient of $S_2(E)$ by the (a priori unknown) subgroup $E(\mathbb{Q})/2E(\mathbb{Q})$ is the **obstruction** to 2-descent, and is equal to $\text{Ш}(E)[2]$, the part of the Tate–Shafarevitch group of E killed by 2.

2-descent quite powerful, basis of Cremona's `mwrank` program. If fails, can try a **second descent** (solve the quartics), or a 3-descent or higher.

Exercise: try your 2-descent skills for $y^2 = x^3 \pm 16$ (both have rank 0).

EXAMPLE OF 3-DESCENT (I)

Not difficult but too long to explain, so we give an interesting example.

Goal: given nonzero integers a, b, and c, determine if there exists a nontrivial solution to $ax^3+by^3+cz^3=0$.

As usual, easy to give condition for everywhere local solubility (see text).

To go further, for any $n\in\mathbb{Z}_{\ge1}$ let E_n be the elliptic curve $y^2=x^3+n^2$. The point $T=(0,n)$ is torsion of order 3. We define a 3-descent map α from $E(\mathbb{Q})$ to $\mathbb{Q}^*/{\mathbb{Q}^*}^3$ by setting $\alpha(\mathcal{O})=1$, $\alpha(T)=4n^2$, and otherwise $\alpha((x,y))=y-n$, all modulo cubes. Easy direct check that α is a **group homomorphism**, kernel easy to compute (not needed here).

Projective curve $\mathcal{C}=\mathcal{C}_{a,b,c}$ with equation $ax^3+by^3+cz^3=0$ closely linked to curve $E=E_{4abc}$ as follows.

EXAMPLE OF 3-DESCENT (II)

Proposition. *Define* $\phi(x, y, z) = (-4abcxyz,\ -4abc(by^3 - cz^3),\ ax^3)$.

1. *The map* ϕ *sends* $\mathcal{C}(\mathbb{Q})$ *into* $E(\mathbb{Q})$ *(in projective coordinates).*
2. *Let* $G = \{(X, Y, Z)\} \in E(\mathbb{Q})$ *such that* $c(Y - 4abcZ) = bZ\lambda^3$ *for some* $\lambda \in \mathbb{Q}^*$. *Then* $\mathrm{Im}(\phi) = \phi(\mathcal{C}(\mathbb{Q}))$ *is equal to* G *together with* $\mathcal{O}$ *if* $c/b \in {\mathbb{Q}^*}^3$, *and* T *if* $b/a \in {\mathbb{Q}^*}^3$ *(and immediate to give preimages).*
3. *The set* $\mathcal{C}(\mathbb{Q})$ *is nonempty if and only if* b/c *modulo cubes belongs to* $\mathrm{Im}(\alpha) \subset \mathbb{Q}^*/{\mathbb{Q}^*}^3$.

Proof: (1) and (2) are simple verifications. For (3), $\mathcal{C}(\mathbb{Q}) \neq \emptyset$ iff $\mathrm{Im}(\phi) \neq \emptyset$, hence iff either there exists $(X, Y, Z) \in E(\mathbb{Q})$ and $\lambda \in \mathbb{Q}^*$ with $c(Y - 4abcZ) = bZ\lambda^3$, or if c/b or b/a are cubes. Note $\lambda = 2cz/x$. This easily implies that $b/c \in \mathrm{Im}(\alpha)$.

EXAMPLE OF 3-DESCENT (III)

Thus, to test solubility of $ax^3 + by^3 + cz^3 = 0$, proceed as follows. First test everywhere local solubility (easy). Then compute the Mordell–Weil group $E(\mathbb{Q})$ using 2-descent and/or a software package like Cremona's `mwrank` (of course may be difficult), also torsion subgroup (easy). If $(P_i)_{1\le i\le r}$ basis of free part, then classes modulo $3E(\mathbb{Q})$ of $P_0 = T$ and the P_i form an $\mathbb{F}_3$-basis of $E(\mathbb{Q})/3E(\mathbb{Q})$. Then check if b/c modulo cubes belongs to the group generated by the $(\alpha(P_i))_{0\le i\le r}$ in $\mathbb{Q}^*/{\mathbb{Q}^*}^3$, simple linear algebra over $\mathbb{F}_3$. Completely algorithmic, **apart from** the MW computations.

EXAMPLE OF 3-DESCENT (IV)

Examples:

- $x^3 + 55y^3 + 66z^3 = 0$. Everywhere locally soluble, cannot solve algebraically as far as I know. Use above method. Find torsion subgroup of order 3 generated by $P_0 = T = (0, 14520)$. In a fraction of a second, `mwrank` (or 2-descent) says rank 1 and a generator $P_1 = (504, 18408)$. Then modulo cubes $\alpha(P_0) = 2^2 \cdot 3^2 \cdot 5^2 \cdot 11$ and $\alpha(P_1) = 2 \cdot 3^2$, while $b/c = 2^2 \cdot 3^2 \cdot 5$. Linear algebra immediately shows b/c **not** in group generated by $\alpha(P_0)$ and $\alpha(P_1)$, so no solution.

EXAMPLE OF 3-DESCENT (V)

- Descent not always negative: $x^3 + 17y^3 + 41z^3 = 0$. Torsion subgroup of order 3 generated by $P_0 = T = (0, 2788)$. Rank 1 and generator $P_1 = (355278000385/2600388036, -42605457792535641 7/132604187507784)$. Modulo cubes $\alpha(P_0) = 17^2.41^2$, $\alpha(P_1) = 17^2$, and $b/c = 17 \cdot 41^2$, so since α group homomorphism, $\alpha(P_0 + P_1) = b/c$ modulo cubes. Find in projective coordinates $P_0 + P_1 = (X, Y, Z) = (594239120333552 2320, 251765584367435734052, 331494724433 2625)$, compute λ such that $c(Y - 4abcZ) = bZ\lambda^3$, find $\lambda = 8363016/149105$. Since $\lambda = 2cz/x$, find (up to projective scaling) $z = 101988$, $x = 149105$, hence $y = 140161$.

THE USE OF $L(E,s)$ (I)

Extremely important method which at least determines whether or not E has nontorsion points, without giving them.

Definition of $L(E,s)$. Assume **minimal Weierstrass equation** over $\mathbb{Q}$. If E has good reduction at p, define $a_p = p+1-|E(\mathbb{F}_p)|$ and $\chi(p)=1$. Otherwise define $\chi(p)=0$, and $a_p=0$ if **triple point** (additive reduction), $a_p=1$ or $a_p=-1$ if **double point** with or without rational tangents (split or nonsplit multiplicative reduction). In fact $a_p = p+1-|E(\mathbb{F}_p)|$ still true. Then

$$L(E,s)=\prod_p \frac{1}{1-a_pp^{-s}+\chi(p)p^{1-2s}}\ ,$$

converges for $\Re(s)>3/2$ because of Hasse bound $|a_p|\le 2p^{1/2}$.

THE USE OF $L(E,s)$ (II)

Most important theorem, due to Wiles, Taylor–Wiles, et al.: $L(E,s)$ extends to a holomorphic function to the whole complex plane, satisfying a functional equation

$$\Lambda(E,2-s)=\varepsilon(E)\Lambda(E,s)\ ,$$

with $\varepsilon(E)=\pm1$ (the root number), and $\Lambda(E,s)=N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$. Here N is the conductor, divisible by all bad primes and easily computable by Tate's algorithm.

Because of BSD, are interested in the value $L(E,1)$. If $\varepsilon(E)=-1$, trivially $L(E,1)=0$. Otherwise, **automatic consequence**, we have the **exponentially convergent** (so **easy to compute**) series

$$L(E,1)=2\sum_{n\geq1}\frac{a_n}{n}e^{-2\pi n/\sqrt{N}}\ .$$

THE USE OF $L(E,s)$ (III)

The Birch and Swinnerton-Dyer conjecture: precise statement, but tells us in particular that there exist nontorsion points in $E(\mathbb{Q})$ (i.e., $E(\mathbb{Q})$ infinite) if and only if $L(E,1)=0$. Unfortunately, except in the rank 1 case (Heegner point method) does not help us much in **finding** the points.

What is known (Rubin, Kolyvagin, etc...):

- If $L(E,1)\neq 0$ then no nontorsion points.

- If $L(E,1)=0$ but $L'(E,1)\neq 0$ then **rank** 1, in particular exists nontorsion points, and can be found using Heegner points.

On the other hand, if $L(E,1)=L'(E,1)=0$, **nothing** known, although BSD conjecture says rank at least 2.

The Heegner point method (I)

This is a remarkable way to use $L(E,s)$ to **find** a nontorsion rational point, works only when the rank is equal to 1 (otherwise always gives a torsion point, even in rank $r \geq 2$).

Tools: complex multiplication and the modular parametrization. For the algorithm, need to understand the theorems, but not the proofs. In fact, **conjectures** are sufficient since checking rational points is trivial.

Setup: E elliptic curve over $\mathbb{Q}$ and $L(E,s) = \sum_{n\geq 1} a_n n^{-s}$.

THE HEEGNER POINT METHOD (II)

Modular parametrization: Wiles's theorem is equivalent to $f_E(\tau) = \sum_{n\geq 1} a_n q^n$ ($q = \exp(2i\pi\tau)$) is a modular form of weight 2 on $\Gamma_0(N)$. Equivalently still, $2i\pi f_E(\tau)d\tau$ is a **holomorphic differential**, invariant under $\Gamma_0(N)$ up to the period lattice of f_E, i.e.,

$$\phi(\tau) = 2i\pi \int_{i\infty}^{\tau} f_E(z)\, dz = \sum_{n\geq 1} \frac{a_n}{n} q^n$$

does not depend on chosen path, and defines map from $\mathcal{H}/\Gamma_0(N)$ to $\mathbb{C}/\Lambda$, easily extended to map from closure $X_0(N)$ to $\mathbb{C}/\Lambda$, where Λ lattice generated by $2i\pi \int_{i\infty}^{\gamma} f_E(z)\, dz$, with $\gamma \in \mathbb{Q}$ a cusp. **Usually** (always happens in practice, if not can easily be dealt with) have $\Lambda \subset \Lambda_E$, with $E(\mathbb{C}) = \mathbb{C}/\Lambda_E$, so get a map from $X_0(N)$ to $\mathbb{C}/\Lambda_E$, and composing with the Weierstrass $\wp$ function, get map φ from $X_0(N)$ to $E(\mathbb{C})$, the modular parametrization. Wiles: exists and unique up to sign.

THE HEEGNER POINT METHOD (III)

Complex multiplication (CM): say τ is a CM point if $\tau \in \mathcal{H}$ is a root of quadratic equation $AX^2 + BX + C = 0$ with A, B, C integral with $B^2 - 4AC < 0$. Make this unique by requiring $\gcd(A, B, C) = 1$ and $A > 0$, then set $\Delta(\tau) = B^2 - 4AC$.

Basic result of CM (in our context): if τ is a **suitable** CM point, then $\varphi(\tau) \in E(H)$ and not only $\varphi(\tau) \in E(\mathbb{C})$, where H is the Hilbert class field of $K = \mathbb{Q}(\sqrt{D})$. This is the **magic** of CM: create **algebraic** numbers using **analytic** functions (Kronecker's dream of youth: do this for other number fields).

THE HEEGNER POINT METHOD (IV)

Assume for simplicity $D = \Delta(\tau)$ discriminant of a quadratic field (fundamental discriminant).

Definition: Given N, τ is a Heegner point of level N if it satisfies the equivalent conditions:

- $\Delta(N\tau) = \Delta(\tau)$
- $N \mid A$ and $\gcd(A/N, B, CN) = 1$
- $N \mid A$ and $D \equiv B^2 \pmod{4N}$.

THE HEEGNER POINT METHOD (V)

Basic properties:

- Let τ Heegner point of level N. If $\gamma \in \Gamma_0(N)$ then $\gamma(\tau)$, $W(\tau) = -1/(N\tau)$, and more generally $W_Q(\tau)$ (Atkin–Lehner operators) are again Heegner points of level N.

- Recall natural correspondence between $SL_2(\mathbb{Z})$ classes of binary quadratic forms and the ideal class group of corresponding quadratic field. This easily generalizes to $\Gamma_0(N)$-equivalence as follows: natural correspondence between $\Gamma_0(N)$-equivalence classes of Heegner points of discriminant D and level N and the set of **pairs** $(\beta, [\mathfrak{a}])$, with $[\mathfrak{a}]$ ideal class, and $\beta \in \mathbb{Z}/2N\mathbb{Z}$ such that $\beta^2 \equiv D \pmod{4N}$.

The Heegner point method (VI)

Main theorem of CM: Let $\tau = (\beta, [\alpha])$ Heegner point of discriminant D (fundamental) and level N, $K = \mathbb{Q}(\sqrt{D})$, H Hilbert class field of K (maximal unramified Abelian extension of K, $\mathrm{Gal}(H/K) \simeq Cl(K)$ through the Artin map Art). Recall φ modular parametrization from $X_0(N)$ to E. Then:

- $\varphi(\tau) \in E(H)$ (algebraicity)

- If $[\mathfrak{b}] \in Cl(K)$ then (Shimura reciprocity):

$$\varphi((\beta, [\mathfrak{a}]))^{\mathrm{Art}([\mathfrak{b}])} = \varphi((\beta, [\mathfrak{a}\mathfrak{b}^{-1}]))$$

Also formula for $\varphi(W((\beta, [\mathfrak{a}])))$ and $\varphi(W_Q((\beta, [\mathfrak{a}])))$.

- $\varphi((-\beta, [\mathfrak{a}]^{-1})) = \overline{\varphi((\beta, [\mathfrak{a}]))}$.

THE HEEGNER POINT METHOD (VII)

Consequence: Can compute the trace of $\varphi(\tau)$ on the elliptic curve by

$$P = \sum_{\sigma\in\mathrm{Gal}(H/K)} \varphi((\beta,[\mathfrak{a}]))^{\sigma} = \sum_{[\mathfrak{b}]\in Cl(K)} \varphi((\beta,[\mathfrak{a}\mathfrak{b}^{-1}])) = \sum_{[\mathfrak{b}]\in Cl(K)} \varphi((\beta,[\mathfrak{b}]))\ ,$$

the sum being computed with the **group law** of E. By Galois theory we will have $P \in E(K)$, so we have considerably reduced the field of definition of the algebraic point on E. In addition, easy result:

If $\varepsilon(E) = -1$ (which is our case since rank 1), then in fact $P \in E(\mathbb{Q})$, which is what we want.

THE HEEGNER POINT METHOD (VII)

Thanks in particular to Gross–Zagier and Kolyvagin, know that P is **nontorsion** if and only if $r = 1$ (already known) **and** $L(E_D, 1) \neq 0$, where E_D is the quadratic twist of E by D (equation $Dy^2 = x^3 + ax + b$).

Point P often **large** multiple of generator, can reduce it considerably again by using Gross–Zagier. Get very nice algorithm.

Example: congruent number problem for $n = 157$, curve $y^2 = x^3 - 157^2x$. Rank 1. Already reasonably large example. In a couple of minutes, find $P = (x, y)$ with numerator and denominator of x having up to 36 decimal digits.

For details on all of this, see student presentation.

COMPUTATION OF INTEGRAL POINTS (I)

Assume now that Mordell–Weil group $E(\mathbb{Q})$ computed, say $(P_i)_{1\le i\le r}$ generators.

Goal: compute $E(\mathbb{Z})$, i.e., **integral points**. Immediate warning: depends on the chosen model, contrary to $E(\mathbb{Q})$.

If $P \in E(\mathbb{Z}) \subset E(\mathbb{Q})$, can write $P = T + \sum_{1\le i\le r} x_i P_i$ with $x_i \in \mathbb{Z}$ and T a torsion point. Easy result is $|x| \ge c_1 e^{c_2 H^2}$, with $H = \max_i |x_i|$ and c_1, c_2 easily computable explicit constants.

Now use elliptic logarithm ψ ($E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$, and ψ maps $P \in E(\mathbb{C})$ to $z \in \mathbb{C}$ modulo Λ such that $(\wp(z), \wp'(z)) = P$).

Computation of integral points (II)

Consequence of above: easy to show that if $|x| \geq c_3$ explicit, then $|\psi(P)| \leq c_5 e^{-c_2 H^2/2}$ (if we choose $\psi(P)$ as small as possible.

On the other hand, thanks to a very important theorem of S. David on linear forms in elliptic logarithms, generalizing Baker-type results to the elliptic case, can prove that we have an inequality for $\psi(P)$ in the other direction, which **contradicts** the above for H sufficiently large. Every constant **explicit**. Thus get **upper bound** for H, and as usual in Baker-type estimates, very large. Typically find $H \leq 10^{100}$ (recall $P = T + \sum_{1 \leq i \leq r} x_i P_i$ and $H = \max_i |x_i|$).

Computation of integral points (II)

In the above, essential that Baker bounds be **explicit**, but **not** essential that they be **sharp** (e.g., 10^{80} or 10^{100} is just as good), because now we use the magic of the LLL algorithm: find small vectors in lattices, and this allows you either to find linear dependence relations between complex numbers, **or** to show that if an approximate relation exists then coefficients are **bounded** very effectively. Roughly obtain a **logarithmic decrease** in the size of the upper bound.

Computation of integral points (III)

Example: $y^2 + y = x^3 - 7x + 6$, famous curve because elliptic curve with smallest conductor of rank 3, important in obtaining effective lower bounds for the class number of imaginary quadratic fields (Goldfeld, Gross–Zagier). Using David's bounds, find $H \leq 10^{60}$. Using LLL once, reduce this spectacularly to $H \leq 51$. Using LLL a second time, reduce this to $H \leq 11$ (diminishing returns: another LLL gives 10, then no improvement). Now a direct search very easy (less than 10000 trials), and find exactly 36 integral points, a very large number.

Phenomenon not completely understood: elliptic curve of high rank with respect to conductor have **many** integral points.