The method of Kraus

Sander Dahmen

VU University Amsterdam

Bilecik, September 9, 2014

Kraus

The modular method can solve certain exponential Diophantine equations for all large enough prime exponents, e.g.:

- $x^p + y^p = z^p, \quad p \geq 5$
- $x^2 = y^p + 2^k z^p, \quad p \geq 7$ (and $k \geq 4$)

Sometimes there are obstructions to do this, e.g. for:

- $x^3 + y^3 = z^p, \quad gcd(x, y, z) = 1$ (1)
  (obstruction: $2^3 + 1^3 = 3^2$)
- $x^2 + 7 = y^p$ (2)
  (obstructions: $11^2 + 7 = 2^7$, $181^2 + 7 = 2^{15}$)

Kraus developed a method that can often be used to solve an equation for a fixed prime exponent p.
He used it to solve (1) for primes p with $17 \leq p \leq 10000$.
Important role in solution of (2) by Bugeaud-Mignotte-Siksek.

$x^2 + 7 = y^p$

We illustrate the method of Kraus by looking at

$$x^2 + 7 = y^p, \quad x, y, p \in \mathbb{Z} \text{ and } p \geq 3.$$

Theorem (Bugeaud-Mignotte-Siksek)

The only solutions to the equation above are the following:

p	3	3	4	5	5	7	15
$\lvert x \rvert$	1	181	3	5	181	11	181
y	2	32	± 2	2	8	2	2

p even is easy and $p \in \{3, 5, 7\}$ can be solved by reducing to Thue equations.
So it remains to solve the equation for primes $p \geq 11$.
We also use Ljunggrens result that y is even.

A Frey curve associated to a solution of $x^2 + 7 = y^p$

We assume (w.l.o.g.) that $p \geq 11$ is prime and $x \equiv 1 \pmod 4$.

Consider the Frey curve:

$$E_x : Y^2 = X^3 + xX^2 + \frac{x^2+7}{4}X$$

This Weierstrass equation has discriminant

$$\begin{aligned} \Delta &= 2^4 \operatorname{Disc}_X \left(X^3 + xX^2 + \frac{x^2+7}{4}X \right) \\ &= -7(x^2+7)^2 = -7y^{2p}. \end{aligned}$$

The *minimal discriminant* $\Delta_{\min}$ and conductor N are:

$$\begin{aligned} \Delta_{\min} &= \frac{\Delta}{2^{12}} = \frac{-7y^{2p}}{2^{12}} \\ N &= \prod_{\text{primes } l \mid 14y} l \end{aligned}$$

Isogenies, level lowering and modularity

- $p \geq 11$ and E_x is semistable (i.e. N is squarefree).
  Mazur: E_x does not have any p-isogenies.
- Recall

$$N_p := N / \prod_{q \in S_p} q$$

  with

$$\begin{aligned} S_p &:= \{\text{primes } q : q || N \text{ and } p | \mathrm{ord}_q(\Delta_{\min}) \\ &= \{\text{primes } q : q | y \text{ and } q \neq 2, 7\}. \end{aligned}$$

  So

$$N_p = 14.$$

- Level lowering (and modularity): There exists a newform f of level 14 such that $E_x \sim_p f$.

Level 14

```
> N:=Newforms(CuspForms(14));
> N;
[* [*
    q - q^2 - 2*q^3 + q^4 + 2*q^6 + q^7 - q^8 + q^9 + O(q^12)
*] *]
> F:=EllipticCurve(N[1,1]);
> F;
Elliptic Curve defined by y^2 + x*y + y = x^3 + 4*x - 6 over
Rational Field
```

So $E_x \sim_p F$, hence for all primes l

- if $l \nmid 14y$, then $a_l(F) \equiv a_l(E_x) \pmod{p}$, and
- if $l \nmid 14$ and $l|y$ then $a_l(F) \equiv \pm(l+1) \pmod{p}$.

Comparing $a_l(E)$ and $a_l(F)$

Now take $p := 37$ and $l := 4 \cdot 37 + 1 = 149$.
If $149 | y$ (which is a priori possible, since $\left(\frac{-7}{149}\right) = 1$), then

$$a_{149}(F) \equiv \pm(149 + 1) \pmod{37}.$$

```
> FrobeniusTraceDirect(F,149);
-18
```

So $a_{149}(F) \equiv -18 \not\equiv \pm 150 \equiv \pm 2 \pmod{37}$, which shows $149 \nmid y$.
This gives $x \not\equiv \pm 80 \pmod{149}$.
Recall that

$$a_{149}(E_x) = 149 + 1 - \#\tilde{E}_x(\mathbb{F}_{149}),$$

so this number only depends on x modulo 149.

Comparing $a_l(E)$ and $a_l(F)$

Possibilities for $a_{149}(E_x)$

```
> alSet:={};
> for x in [X : X in [0..148] | not X in {80,69}] do
for>   E:=EllipticCurve([0,x,0,(x^2+7)/4,0]);
for>   al:=FrobeniusTraceDirect(E,149);
for>   alSet:=alSet join {al};
for> end for;
> alSet;
{ -22, -18, -14, -10, -6, -2, 2, 6, 10, 14, 18, 22 }
```

So $a_{149}(E_x) \in \{-22, -18, -14, -10, -6, -2, 2, 6, 10, 14, 18, 22\}$
Recall $a_{149}(F) = -18$, so no contradiction.
Bound to happen, since E_{-11} and E_{181} have conductor 11.
So if $x \equiv -11$ or 181 (mod 149), then $a_{149}(E_x) = a_{149}(F)$.

Comparing $a_l(E)$ and $a_l(F)$

Use $x^2 + 7 \equiv y^{37} \pmod{149}$ to restrict possibilites for x!
Note $\mathbb{F}_{149}^*$ is cyclic of order $149 - 1 = 4 * 37$. So

$$\left\{\overline{y}^{37} : \overline{y} \in \mathbb{F}_{149}^*\right\} = \left\{\zeta \in \mathbb{F}_{149}^* : \zeta^4 = 1\right\} = \{\pm 1, \pm 44\}$$

Now

$$x^2 + 7 \equiv \pm 1, \pm 44 \pmod{149}$$

This gives

$$x \equiv \pm 21, \pm 22 \pmod{149}$$

Possible $a_{149}(E_x)$ for these x are:

$$a_{149}(E_x) \in \{6, 22\}$$

This contradicts $a_{149}(F) \equiv a_{149}(E_x) \pmod{37}$.
So no integer solutions to $x^2 + 7 = y^p$ for $p = 37$.

General primes $p \geq 11$

Let $n \in \mathbb{Z}_{>0}$ such that $l := np + 1$ is prime
If $\left(\frac{-7}{l}\right) = -1$, then $l \nmid y$.
If $\left(\frac{-7}{l}\right) = 1$, then compute $a_l(F)$. Assuming $l|y$, we have

$$a_l(F) \equiv \pm(l+1) \equiv \pm(np+2) \equiv \pm 2 \pmod{p}.$$

Conclusion: If $\left(\frac{-7}{l}\right) = -1$ or $a_l(F)^2 \not\equiv 4 \pmod{p}$ then $l \nmid y$.
Assuming $l \nmid y$, we have that y^p modulo l is contained in

$$\{\overline{y}^p : \overline{y} \in \mathbb{F}_l^*\} = \{\zeta \in \mathbb{F}_l^* : \zeta^n = 1\} =: \mu_n(\mathbb{F}_l)$$

So x modulo l is contained in

$$\{\overline{x} \in \mathbb{F}_l : \overline{x}^2 + 7 \in \mu_n(\mathbb{F}_l)\} =: X(n, l)$$

If for all $\overline{x} \in X(n, l)$ we have

$$a_l(E_{\overline{x}}) \not\equiv a_l(F) \pmod{p}$$

then there are no solutions with $l \nmid y$.

To summarize

$$F : Y^2 + X * Y + Y = X^3 + 4 * X - 6$$
$$\mu_n(\mathbb{F}_l) := \{\zeta \in \mathbb{F}_l^* : \zeta^n = 1\}$$
$$X(n, l) := \{\overline{x} \in \mathbb{F}_l : \overline{x}^2 + 7 \in \mu_n(\mathbb{F}_l)\}$$

Theorem (Cremona-Siksek)

Let $p \geq 11$ be prime. If there exists an $n \in \mathbb{Z}_{>0}$ such that

- *$l := np + 1$ is prime, and*
- *$\left(\frac{-7}{l}\right) = -1$ or $a_l(F)^2 \not\equiv 4 \pmod{p}$, and*
- *for all $\overline{x} \in X(n, l)$ we have*

$$a_l(F) \not\equiv a_l(E_{\overline{x}}) \pmod{p}.$$

Then there are no integer solutions to $x^2 + 7 = y^p$.

Conditions are satisfied for all $11 \leq p \leq 181\ 000\ 000$.