Techniques for Solving Diophantine Equations

Carmen Bruni

November 29th, 2012

What is a Diophantine Equation?

A Diophantine equation is a polynomial equation over $\mathbb{Z}$ in n variables in which we look for integer solutions (some people extend the definition to include any equation where we look for integer solutions). We ideally wish to classify all integer solutions to these equations.

What is a Diophantine Equation?

A Diophantine equation is a polynomial equation over $\mathbb{Z}$ in n variables in which we look for integer solutions (some people extend the definition to include any equation where we look for integer solutions). We ideally wish to classify all integer solutions to these equations.

Who cares?

Why Study Diophantine Equations?

Why Study Diophantine Equations?

- It's a fun challenge.

Why Study Diophantine Equations?

- It's a fun challenge.
- It gives justification for other studying subjects (for example algebraic number theory or algebraic geometry).

Why Study Diophantine Equations?

- It's a fun challenge.
- It gives justification for other studying subjects (for example algebraic number theory or algebraic geometry).
- It leads to other interesting questions.

Why Study Diophantine Equations?

- It's a fun challenge.
- It gives justification for other studying subjects (for example algebraic number theory or algebraic geometry).
- It leads to other interesting questions. For example
  - Pell equations, $x^2 - dy^2 = 1$, lead to questions about continued fractions and fundamental units.

Why Study Diophantine Equations?

- It's a fun challenge.
- It gives justification for other studying subjects (for example algebraic number theory or algebraic geometry).
- It leads to other interesting questions. For example
  - Pell equations, $x^2 - dy^2 = 1$, lead to questions about continued fractions and fundamental units.
  - Ljunggren's equation $A^4 - 2B^2 = 8$ is related to approximations of π.

Why Study Diophantine Equations?

- It's a fun challenge.
- It gives justification for other studying subjects (for example algebraic number theory or algebraic geometry).
- It leads to other interesting questions. For example
  - Pell equations, $x^2 - dy^2 = 1$, lead to questions about continued fractions and fundamental units.
  - Ljunggren's equation $A^4 - 2B^2 = 8$ is related to approximations of π.
  - Fermat's Last Theorem $x^n + y^n = z^n$ lead to questions about unique factorization domains, cyclotomic fields, elliptic curves and modular forms.

Philosophy of Diophantine Equations

Philosophy of Diophantine Equations

It is easier to show that a Diophantine Equations has no solutions than it is to solve an equation with a solution.

Technique 1. Local obstructions

Technique 1. Local obstructions

Theorem

The equation $x^2 - 3y^2 = 175$ *has no solutions in integers* x *and* y*.*

Technique 1. Local obstructions

Theorem

The equation $x^2 - 3y^2 = 175$ has no solutions in integers x and y.

Proof.

Assume we have a solution in x and y.

Technique 1. Local obstructions

Theorem

The equation $x^2 - 3y^2 = 175$ has no solutions in integers x and y.

Proof.

Assume we have a solution in x and y. What we will do is look locally at 4, that is consider the equation over $\mathbb{Z}_4$. Then, the equation becomes $x^2 + y^2 = 3 \pmod 4$.

Technique 1. Local obstructions

Theorem

The equation $x^2 - 3y^2 = 175$ has no solutions in integers x and y.

Proof.

Assume we have a solution in x and y. What we will do is look locally at 4, that is consider the equation over $\mathbb{Z}_4$. Then, the equation becomes $x^2 + y^2 = 3 \pmod 4$. Now, notice that

$$0^2 \equiv 0 \pmod 4 \qquad 1^2 \equiv 1 \pmod 4$$
$$2^2 \equiv 0 \pmod 4 \qquad 3^2 \equiv 1 \pmod 4$$

and hence the only squares in $\mathbb{Z}_4$ are 0 and 1.

Technique 1. Local obstructions

Theorem

The equation $x^2 - 3y^2 = 175$ has no solutions in integers x and y.

Proof.

Assume we have a solution in x and y. What we will do is look locally at 4, that is consider the equation over $\mathbb{Z}_4$. Then, the equation becomes $x^2 + y^2 = 3 \pmod 4$. Now, notice that

$$0^2 \equiv 0 \pmod 4 \qquad 1^2 \equiv 1 \pmod 4$$
$$2^2 \equiv 0 \pmod 4 \qquad 3^2 \equiv 1 \pmod 4$$

and hence the only squares in $\mathbb{Z}_4$ are 0 and 1. Notice that the sum of any two squares is either 0, 1 or 2. But our equation reduced to the sum of two squares with value 3, a contradiction.

Technique 1. Local obstructions

Question: How powerful is this technique? Will it always work?

Technique 1. Local obstructions

Question: How powerful is this technique? Will it always work?

- If the equation has a solution then this technique will never work as we will always have local solutions (just use the solution over $\mathbb{Z}$ and project down).

Technique 1. Local obstructions

Question: How powerful is this technique? Will it always work?

- If the equation has a solution then this technique will never work as we will always have local solutions (just use the solution over $\mathbb{Z}$ and project down).
- What if the equation has no solution. Must there be a prime p such that over $\mathbb{Z}_p$ our equation has no solution?

Technique 1. Local obstructions

Question: How powerful is this technique? Will it always work?

- If the equation has a solution then this technique will never work as we will always have local solutions (just use the solution over $\mathbb{Z}$ and project down).
- What if the equation has no solution. Must there be a prime p such that over $\mathbb{Z}_p$ our equation has no solution?

No!

Technique 1. Local obstructions

Question: How powerful is this technique? Will it always work?

- If the equation has a solution then this technique will never work as we will always have local solutions (just use the solution over $\mathbb{Z}$ and project down).
- What if the equation has no solution. Must there be a prime p such that over $\mathbb{Z}_p$ our equation has no solution?

No!

Definition

An equation is said to satisfy the Hasse Principle (local to global principle) if whenever it has a solution over $\mathbb{R}$ and over every $\mathbb{Z}_p$, then it has one over $\mathbb{Z}$.

Technique 1. Local obstructions

Question: How powerful is this technique? Will it always work?

- If the equation has a solution then this technique will never work as we will always have local solutions (just use the solution over $\mathbb{Z}$ and project down).
- What if the equation has no solution. Must there be a prime p such that over $\mathbb{Z}_p$ our equation has no solution?

No!

Definition

An equation is said to satisfy the Hasse Principle (local to global principle) if whenever it has a solution over $\mathbb{R}$ and over every $\mathbb{Z}_p$, then it has one over $\mathbb{Z}$.

There exist equations that do not satisfy the Hasse Principle!

Counter Examples to the Hasse Principle

Theorem (Selmer 1951)

The equation

$$3x^3 + 4y^3 + 5z^3 = 0$$

has solutions over $\mathbb{R}$ and in $\mathbb{Z}_p$ for every prime p but does not have a solution over $\mathbb{Z}$.

Counter Examples to the Hasse Principle

Theorem (Selmer 1951)

The equation

$$3x^3 + 4y^3 + 5z^3 = 0$$

has solutions over $\mathbb{R}$ and in $\mathbb{Z}_p$ for every prime p but does not have a solution over $\mathbb{Z}$.

The proof of this is a bit tricky. If we remove the requirement that we have a real solution, we can come up with a very nice counter example.

Counter Examples to the Hasse Principle

Theorem

The equation

$$w^2 + x^2 + y^2 + z^2 = -1$$

has solutions in $\mathbb{Z}_p$ for every prime p but does not have a solution over $\mathbb{Z}$.

Counter Examples to the Hasse Principle

Theorem

The equation

$$w^2 + x^2 + y^2 + z^2 = -1$$

has solutions in $\mathbb{Z}_p$ for every prime p but does not have a solution over $\mathbb{Z}$.

Proof.

No Solutions over $\mathbb{Z}$:

Counter Examples to the Hasse Principle

Theorem

The equation

$$w^2 + x^2 + y^2 + z^2 = -1$$

has solutions in $\mathbb{Z}_p$ for every prime p but does not have a solution over $\mathbb{Z}$.

Proof.

No Solutions over $\mathbb{Z}$: Exercise

Counter Examples to the Hasse Principle

Theorem

The equation

$$w^2 + x^2 + y^2 + z^2 = -1$$

has solutions in $\mathbb{Z}_p$ for every prime p but does not have a solution over $\mathbb{Z}$.

Proof.

No Solutions over $\mathbb{Z}$: Exercise

Solutions in $\mathbb{Z}_p$: Reducing modulo p gives

$$w^2 + x^2 + y^2 + z^2 = -1 \equiv p - 1 \pmod{p}$$

Counter Examples to the Hasse Principle

Theorem

The equation

$$w^2 + x^2 + y^2 + z^2 = -1$$

has solutions in $\mathbb{Z}_p$ for every prime p but does not have a solution over $\mathbb{Z}$.

Proof.

No Solutions over $\mathbb{Z}$: Exercise

Solutions in $\mathbb{Z}_p$: Reducing modulo p gives

$$w^2 + x^2 + y^2 + z^2 = -1 \equiv p - 1 \pmod{p}$$

Since $p - 1 \geq 0$, we invoke Lagrange's theorem on sums of four squares which says that every non-negative integer can be written as a sum of four squares of integers and conclude the result.

Technique 2. Algebraic Number Theory Techniques

We are looking for solutions over $\mathbb{Z}$ to Diophantine Equations. What, if any of these properties still hold for other rings?

Technique 2. Algebraic Number Theory Techniques

We are looking for solutions over $\mathbb{Z}$ to Diophantine Equations. What, if any of these properties still hold for other rings?

- A early attempt on Fermat's Last Theorem $x^n + y^n = z^n$ involved using the ring of integers of the cyclotomic field $\mathbb{Z}[\zeta_n]$ where $\zeta_n^n = 1$ and attempting to factor the equation.

Technique 2. Algebraic Number Theory Techniques

We are looking for solutions over $\mathbb{Z}$ to Diophantine Equations. What, if any of these properties still hold for other rings?

- A early attempt on Fermat's Last Theorem $x^n + y^n = z^n$ involved using the ring of integers of the cyclotomic field $\mathbb{Z}[\zeta_n]$ where $\zeta_n^n = 1$ and attempting to factor the equation.
- The biggest obstacle in this attempt was that $\mathbb{Z}[\zeta_n]$ is not always a unique factorization domain! (In fact erroneous proofs of FLT appeared in the literature which assumed this fact).

Technique 2. Algebraic Number Theory Techniques

We are looking for solutions over $\mathbb{Z}$ to Diophantine Equations. What, if any of these properties still hold for other rings?

- A early attempt on Fermat's Last Theorem $x^n + y^n = z^n$ involved using the ring of integers of the cyclotomic field $\mathbb{Z}[\zeta_n]$ where $\zeta_n^n = 1$ and attempting to factor the equation.
- The biggest obstacle in this attempt was that $\mathbb{Z}[\zeta_n]$ is not always a unique factorization domain! (In fact erroneous proofs of FLT appeared in the literature which assumed this fact).
- Perhaps if we look at rings with unique factorization (or even better - if we look at Euclidean domains) we can extend some of factorization techniques.

Theorem (Fermat's theorem on sums of two squares)

We have that $p = x^2 + y^2$ *for a prime* p *if and only if* $p \equiv 1 \pmod 4$.

Theorem (Fermat's theorem on sums of two squares)

We have that $p = x^2 + y^2$ for a prime p if and only if $p \equiv 1 \pmod 4$.

Proof.

If $p \equiv 3 \pmod 4$, then our argument from before shows that $p = x^2 + y^2$ has no solutions. So we suppose that $p \equiv 1 \pmod 4$.

Theorem (Fermat's theorem on sums of two squares)

We have that $p = x^2 + y^2$ for a prime p if and only if $p \equiv 1 \pmod 4$.

Proof.

If $p \equiv 3 \pmod 4$, then our argument from before shows that $p = x^2 + y^2$ has no solutions. So we suppose that $p \equiv 1 \pmod 4$. Since $\mathbb{Z}_p^*$ is cyclic, it has a generator say g with $g^{p-1} \equiv 1 \pmod p$. Thus, $g^{(p-1)/2} \equiv -1 \pmod p$ and so there exists an integer, namely $m = g^{(p-1)/4}$, such that $p \mid m^2 + 1$ (notice this fails if $p \equiv 3 \pmod 4$).

Theorem (Fermat's theorem on sums of two squares)

We have that $p = x^2 + y^2$ for a prime p if and only if $p \equiv 1 \pmod 4$.

Proof.

If $p \equiv 3 \pmod 4$, then our argument from before shows that $p = x^2 + y^2$ has no solutions. So we suppose that $p \equiv 1 \pmod 4$. Since $\mathbb{Z}_p^*$ is cyclic, it has a generator say g with $g^{p-1} \equiv 1 \pmod p$. Thus, $g^{(p-1)/2} \equiv -1 \pmod p$ and so there exists an integer, namely $m = g^{(p-1)/4}$, such that $p \mid m^2 + 1$ (notice this fails if $p \equiv 3 \pmod 4$). Look at this over $\mathbb{Z}[i]$, which says that p divides $m^2 + 1 = (m + i)(m - i)$. If p were prime, then p would divide one of $m \pm i$ over $\mathbb{Z}[i]$. Then $p(a + bi) = m \pm i$ and so $pb = \pm 1$ a contradiction since $b \in \mathbb{Z}$. Thus, p is reducible in $\mathbb{Z}[i]$. (Continued on next slide)

Proof.

Recap: $p \equiv 1 \pmod 4$ implies that p is reducible in $\mathbb{Z}[i]$.

Proof.

Recap: $p \equiv 1 \pmod 4$ implies that p is reducible in $\mathbb{Z}[i]$.

Now, Let $N(a+bi) = a^2 + b^2 = |a+bi|^2$ and suppose that $p = wz$ with $w, z \in \mathbb{Z}[i]$ and $w, z \neq \pm 1, \pm i$ (these are the units of $\mathbb{Z}[i]$). Taking the norms of both sides gives $p^2 = N(w)N(z)$.

Proof.

Recap: $p \equiv 1 \pmod 4$ implies that p is reducible in $\mathbb{Z}[i]$.

Now, Let $N(a+bi) = a^2 + b^2 = |a+bi|^2$ and suppose that $p = wz$ with $w, z \in \mathbb{Z}[i]$ and $w, z \neq \pm 1, \pm i$ (these are the units of $\mathbb{Z}[i]$). Taking the norms of both sides gives $p^2 = N(w)N(z)$. This means that either one of the elements has norm 1 which means that it is one of $\pm 1, \pm i$, a contradiction or that each element has norm p. Writing $w = x + iy$, we see that $p = N(w) = x^2 + y^2$ as required.

Technique 3. Linear Forms in Logarithms

Theorem (Baker 1966)

Let $\alpha_1, .., \alpha_n$ be algebraic integers (roots of monic polynomials) and let H be a number larger than the absolute value of the coefficients of the minimum polynomials of the α_i. Let $b_i \in \mathbb{Z}^*$ and let $B = \max_i |b_i|$. Let

$$\Lambda := |\sum_{i=1}^{n} b_i \log \alpha_i|$$

and suppose that $\Lambda \neq 0$.

Theorem (Baker 1966)

Let $\alpha_1, .., \alpha_n$ be algebraic integers (roots of monic polynomials) and let H be a number larger than the absolute value of the coefficients of the minimum polynomials of the α_i. Let $b_i \in \mathbb{Z}^*$ and let $B = \max_i |b_i|$. Let

$$\Lambda := |\sum_{i=1}^{n} b_i \log \alpha_i|$$

and suppose that $\Lambda \neq 0$. Then there exist computable constants C and D so that

$$\Lambda > exp(-L(\log H)^n \log(\log H)^{n-1} \log B)$$

where $L = (Cnd)^{Dn}$ and $d = [\mathbb{Q}(\alpha_1, .., \alpha_n) : \mathbb{Q}]$.

Technique 3. Linear Forms in Logarithms

Technique 3. Linear Forms in Logarithms

Today, under slight modifications to the above statement, Matveev has shown that we can take L to be

$$L := 2 \cdot 30^{n+4}(n+1)^6 d^{n+2}(d+1).$$

Technique 3. Linear Forms in Logarithms

Today, under slight modifications to the above statement, Matveev has shown that we can take L to be

$$L := 2 \cdot 30^{n+4}(n+1)^6 d^{n+2}(d+1).$$

A similar statement even holds for $\Lambda = \left| \prod_{i=1}^{n} \alpha_i^{b_i} - 1 \right|$.

Technique 3. Linear Forms in Logarithms

Today, under slight modifications to the above statement, Matveev has shown that we can take L to be

$$L := 2 \cdot 30^{n+4}(n+1)^6 d^{n+2}(d+1).$$

A similar statement even holds for $\Lambda = \left| \prod_{i=1}^{n} \alpha_i^{b_i} - 1 \right|$.

What can we prove with this theorem?

Technique 3. Linear Forms in Logarithms

Today, under slight modifications to the above statement, Matveev has shown that we can take L to be

$$L := 2 \cdot 30^{n+4}(n+1)^6 d^{n+2}(d+1).$$

A similar statement even holds for $\Lambda = \left| \prod_{i=1}^{n} \alpha_i^{b_i} - 1 \right|$.

What can we prove with this theorem?

Theorem

Let $a, b, k \in \mathbb{Z}$ with $a, b > 1$ and k nonzero. If $a^m - b^n = k$ for $m, n \in \mathbb{Z}$, then m and n are bounded by a computable number depending only on k and the greatest prime divisor of ab.

Technique 3. Linear Forms in Logarithms

The proof to the previous theorem follows from this corollary:

The proof to the previous theorem follows from this corollary:

Theorem

Let P be the set of all the primes up to $M \in \mathbb{N}$. Define

$$S := \left\{ \prod_{p_i \in P} p_i^{a_i} : a_i \in \mathbb{N} \right\}.$$

Order the elements of S by $0 < n_1 < n_2 < \ldots$. Then there exists a computable number C depending on M only so that

$$n_{i+1} - n_i \geq \frac{n_i}{(\log n_i)^C}$$

Proof.

Let $n_i = \prod_{p_i \in P} p_i^{a_i}$ and $n_{i+1} = \prod_{p_i \in P} p_i^{b_i}$. Look at

$$\frac{n_{i+1}}{n_i} - 1 = \prod_{p_i \in P} p_i^{b_i - a_i} - 1$$

Proof.

Let $n_i = \prod_{p_i \in P} p_i^{a_i}$ and $n_{i+1} = \prod_{p_i \in P} p_i^{b_i}$. Look at

$$\frac{n_{i+1}}{n_i} - 1 = \prod_{p_i \in P} p_i^{b_i - a_i} - 1$$

The exponents are bounded by $4 \log n_i$, the primes are bounded by M. Applying our bounds on linear forms in logarithms shows that

$$\frac{n_{i+1}}{n_i} - 1 \geq (\log n_i)^{-C}$$

for some computable C depending only on M.

□

Technique 4. The Modular Method

This technique is best showed by an example. Let's solve FLT, that is, there are no solutions to the equation $x^n + y^n = z^n$ in pairwise coprime integers x, y, z and $n \geq 3$.

Technique 4. The Modular Method

This technique is best showed by an example. Let's solve FLT, that is, there are no solutions to the equation $x^n + y^n = z^n$ in pairwise coprime integers x, y, z and $n \geq 3$. Without loss of generality, suppose n is prime and $n \geq 5$.

Technique 4. The Modular Method

This technique is best showed by an example. Let's solve FLT, that is, there are no solutions to the equation $x^n + y^n = z^n$ in pairwise coprime integers x, y, z and $n \geq 3$. Without loss of generality, suppose n is prime and $n \geq 5$. The techniques here use elliptic curves, modular forms, and a whole lot of machinery.

Definition

An elliptic curve over $\mathbb{Q}$ is any smooth curve (no double roots) satisfying

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in \mathbb{Q}$. By clearing denominators and relabeling, we may assume $a_i \in \mathbb{Z}$.

Technique 4. The Modular Method

Associated to each elliptic curve $y^2 = x^3 + a_2x^2 + a_4x + a_6$ is a number N called the conductor and another number Δ called the discriminant (much like the discriminant of a quadratic or a cubic). These values tell you when the curve is also defined over $\mathbb{F}_p$.

Technique 4. The Modular Method

Associated to each elliptic curve $y^2 = x^3 + a_2x^2 + a_4x + a_6$ is a number N called the conductor and another number Δ called the discriminant (much like the discriminant of a quadratic or a cubic). These values tell you when the curve is also defined over $\mathbb{F}_p$. For example, $y^2 = x^3 + x^2 + 4x + 4$ has conductor $N = 20 = 2^2 \cdot 5$. This elliptic curve is defined in all $\mathbb{F}_p$ where $p \neq 2, 5$. Reducing the curve modulo 5 for example gives

$$y^2 = x^3 + x^2 + 4x + 4 \equiv x^3 + x^2 - x - 1 \equiv (x+1)^2(x-1) \pmod 5$$

which has a double root and hence is not smooth.

Technique 4. The Modular Method

Associated to each elliptic curve $y^2 = x^3 + a_2x^2 + a_4x + a_6$ is a number N called the conductor and another number Δ called the discriminant (much like the discriminant of a quadratic or a cubic). These values tell you when the curve is also defined over $\mathbb{F}_p$. For example, $y^2 = x^3 + x^2 + 4x + 4$ has conductor $N = 20 = 2^2 \cdot 5$. This elliptic curve is defined in all $\mathbb{F}_p$ where $p \neq 2, 5$. Reducing the curve modulo 5 for example gives

$$y^2 = x^3 + x^2 + 4x + 4 \equiv x^3 + x^2 - x - 1 \equiv (x+1)^2(x-1) \pmod 5$$

which has a double root and hence is not smooth.

- Wiles (et al.) showed that newforms are a generalization of elliptic curves. The conductor of an elliptic curve corresponds to something called the level of a modular form.

Technique 4. The Modular Method

Associated to each elliptic curve $y^2 = x^3 + a_2x^2 + a_4x + a_6$ is a number N called the conductor and another number Δ called the discriminant (much like the discriminant of a quadratic or a cubic). These values tell you when the curve is also defined over $\mathbb{F}_p$. For example, $y^2 = x^3 + x^2 + 4x + 4$ has conductor $N = 20 = 2^2 \cdot 5$. This elliptic curve is defined in all $\mathbb{F}_p$ where $p \neq 2, 5$. Reducing the curve modulo 5 for example gives

$$y^2 = x^3 + x^2 + 4x + 4 \equiv x^3 + x^2 - x - 1 \equiv (x+1)^2(x-1) \pmod 5$$

which has a double root and hence is not smooth.

- Wiles (et al.) showed that newforms are a generalization of elliptic curves. The conductor of an elliptic curve corresponds to something called the level of a modular form.
- Ribet showed that newforms with [minimal] discriminants that have very high prime powers in their exponents can be associated to newforms with lower levels.

Technique 4. The Modular Method

Associated to each elliptic curve $y^2 = x^3 + a_2x^2 + a_4x + a_6$ is a number N called the conductor and another number Δ called the discriminant (much like the discriminant of a quadratic or a cubic). These values tell you when the curve is also defined over $\mathbb{F}_p$. For example, $y^2 = x^3 + x^2 + 4x + 4$ has conductor $N = 20 = 2^2 \cdot 5$. This elliptic curve is defined in all $\mathbb{F}_p$ where $p \neq 2, 5$. Reducing the curve modulo 5 for example gives

$$y^2 = x^3 + x^2 + 4x + 4 \equiv x^3 + x^2 - x - 1 \equiv (x+1)^2(x-1) \pmod 5$$

which has a double root and hence is not smooth.

- Wiles (et al.) showed that newforms are a generalization of elliptic curves. The conductor of an elliptic curve corresponds to something called the level of a modular form.
- Ribet showed that newforms with [minimal] discriminants that have very high prime powers in their exponents can be associated to newforms with lower levels.
- The smallest level for a newform is $N = 11$.

Technique 4. The Modular Method

- We 'prove' FLT. Suppose that $a^p + b^p = c^p$ for $a, b, c \in \mathbb{Z}$ pairwise coprime and nonzero and $p \geq 5$ prime. WLOG b is even.

Technique 4. The Modular Method

- We 'prove' FLT. Suppose that $a^p + b^p = c^p$ for $a, b, c \in \mathbb{Z}$ pairwise coprime and nonzero and $p \geq 5$ prime. WLOG b is even.
- Associate to this solution an elliptic curve

$$Y^2 = X(X - a^p)(X + b^p)$$

Technique 4. The Modular Method

- We 'prove' FLT. Suppose that $a^p + b^p = c^p$ for $a, b, c \in \mathbb{Z}$ pairwise coprime and nonzero and $p \geq 5$ prime. WLOG b is even.
- Associate to this solution an elliptic curve

$$Y^2 = X(X - a^p)(X + b^p)$$

- The [minimal] discriminant and conductor are of the form

$$\Delta = 2^{-8}(abc)^{2p} \qquad N = 2 \prod_{q \neq 2, q \mid abc} q$$

Technique 4. The Modular Method

- We 'prove' FLT. Suppose that $a^p + b^p = c^p$ for $a, b, c \in \mathbb{Z}$ pairwise coprime and nonzero and $p \geq 5$ prime. WLOG b is even.
- Associate to this solution an elliptic curve

$$Y^2 = X(X - a^p)(X + b^p)$$

- The [minimal] discriminant and conductor are of the form

$$\Delta = 2^{-8}(abc)^{2p} \qquad N = 2 \prod_{q \neq 2, q \mid abc} q$$

- Since all elliptic curves are modular (that is, they are newforms), and our discriminant has integers to very high exponential powers, we use Ribet's level lowering theorem to find a newform at level $N = 2$. But there are no newforms of level 2! This completes the proof.

Other Techniques

- Skolem's Method

Other Techniques

- Skolem's Method
- Chabauty's Method

Other Techniques

- Skolem's Method
- Chabauty's Method
- Hyper Geometric Method

Other Techniques

- Skolem's Method
- Chabauty's Method
- Hyper Geometric Method
- The Brauer-Manin Obstruction

Other Techniques

- Skolem's Method
- Chabauty's Method
- Hyper Geometric Method
- The Brauer-Manin Obstruction
- The Descent Obstruction

Thank you!