# Diophantine Equations

Manisha Kulkarni

IIIT, Bangalore

June 25, 2012

# Outline

- **Introduction**
- Diophantine equations of the type $f(x) = g(y)$
- Current Research in Diophantine Equations

# Introduction

- Theory of Diophantine equations is a branch of Number Theory which deals with the solutions of polynomial equations in either integers or rational numbers.

◇ $3x + 7 = y$

◇ $x^2 + 18x + 81 = y^2$

◇ $x^2 + y^2 = z^2$, where $x, y$ and $z$ are positive integers.

- ◇ The famous Pythagorean triples $(3, 4, 5)$, $(5, 12, 13)$ etc.
- ◇ $x = k(n^2 - m^2)$, $y = 2knm$, $z = k(n^2 + m^2)$ generates all Pythagorean triples
- ◇ $n = 2, m = 1, k = 1$ gives $x = 3$, $y = 4$, $z = 5$

# Characteristics of Diophantine Equations

- Easy to state
- Extremely difficult to guess if it is trivial to solve or needs deep mathematics
- No general method to solve

# Example : Fermat's Last Theorem

## Theorem

*If $n \geq 3$ is an integer then the equation*

$$x^n + y^n = z^n$$

*does not have any solutions $x, y, z$ in nonzero positive Integers.*

*In other words, the only solutions in rational numbers of the equation $x^n + y^n = 1$ have either $x = 0$ or $y = 0$.*

- Unsolved for more than 350 years
- Proved by Andrew Wiles in 1994 using Algebraic Geometry, Modular forms, Algebraic Number Theory

# Example : Elliptic Curves

- Curves given by cubic equations of the form

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

  such that the roots of $f(x)$ are different.
- Think of an Elliptic Curve as a set of solutions $(x, y)$ to its equation together with an extra point $O$ (*point at infinity*)

# Outline

- Introduction
- **Diophantine equations of the type $f(x) = g(y)$**
- Current Research in Diophantine Equations

# Problem Statement

Diophantine equations of the form $f(x) = g(y)$ where $f(x)$ and $g(y)$ are polynomials with integer or rational coefficients.

Does the equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator?

The equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator if there exists a positive integer $\Delta$ such that $f(x) = g(y)$ has infinitely many rational solutions $x,\ y$ satisfying $\Delta x, \Delta y \in Z$.

# Motivation

- Erdos and Selfridge(1975) : Finite product of consecutive integers can never be a perfect power. In other words, the Diophantine equation

$$x(x+1)(x+2)\cdots(x+m-1) = y^n$$

does not have any nontrivial solution in integers when $m,\ n > 1$.

# Generalization and Finiteness

This leads to the general problem

$$x(x+1)(x+2)\cdots(x+m-1)+r=y^n$$

where $r$ is any rational number.

Surprisingly, except for the two values of $r \in \{1, 1/4\}$, we get that this equation has only finitely many solutions.

**Theorem (With B. Sury and Y. Bilu (Acta Arithmetica))**

*Let $r$ be a nonzero rational number which is not a perfect power in $Q$. Then the equation $x(x+1)(x+2)\cdots(x+m-1)+r=y^n$ has at most finitely many solutions $(x,\ y,\ m,\ n)$ satisfying $(x,\ m,\ n)\in Z$ and $y\in Q$, $m,\ n\geq 2$. Moreover, all the solutions can be calculated effectively.*

## Outline of proof

- $x(x+1)(x+2)\cdots(x+m-1)+r=y^n$

– Used Schinzel - Tijdeman theorem to get bounds on $x, y$ and $n$.

– Bound on $m$ using elementary methods.

# Schinzel - Tijdeman Theorem

In $f(x) = g(y)$ when $g(y) = y^n$, one can use Schinzel - Tijdeman Theorem and get the result.

**Schinzel - Tijdeman's Theorem.**

$f(x) \in Q[x]$ has at least three simple roots and $n > 1$ or $f(x)$ has at least two simple roots and $n > 2$. Then $f(x) = y^n$ has only finitely many solutions in $x \in Z$, $y \in Q$.

Also there exists an effective constant $N(f)$ such that for any solution of $f(x) = y^n$ in $x, \; n \in Z$, $y \in Q$ satisfies $n \leq N(f)$. (Note that here $n$ is variable)

# Bilu - Tichy

In Diophantine equation $x(x+1)(x+2)\cdots(x+m-1)+r=y^n$, we applied Schinzel - Tijdeman theorem to get finiteness of $x$, $y$ and $n$.

However, one can not apply Schinzel - Tijdeman if $g(y)$ is not of the form $y^n$.

In 2000, Bilu and Tichy gave a remarkable theorem in which they obtained explicit finiteness criterion for the equation $f(x)=g(y)$.

- five families of pairs of polynomials $(f,g)$ such that $f(x)=g(y)$ has infinitely many solutions.
- each pair $(f,g)$ for which $f(x)=g(y)$ has infinitely many solutions with bounded denominator can be determined from the above pairs (standard pairs).

**Bilu - Tichy Theorem.**

For non-constant polynomials $f(x)$ and $g(x) \in \mathbf{Q}[x]$, the following are equivalent:

- The equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator.
- We have $f = \phi(f_1(\lambda))$ and $g = \phi(g_1(\mu))$ where $\lambda(x), \mu(x) \in \mathbf{Q}[X]$ are linear polynomials, $\phi(x) \in \mathbf{Q}[X]$, and $(f_1(x), g_1(x))$ is a standard pair over $\mathbf{Q}$ such that the equation $f_1(x) = g_1(y)$ has infinitely many rational solutions with a bounded denominator.

# $x(x+1)(x+2)\cdots(x+m-1) = g(y)$

- $x(x+1)(x+2)\cdots(x+m-1) = g(y)$ ,

– Bilu - Tichy to get finiteness of $x$ and $y$.

– Proved that $m$ is bounded.

# $x(x+1)(x+2)\cdots(x+m-1) = g(y)$

**Theorem (With B. Sury (Indigationes Mathematicae))**

- *Fix $m \geq 3$ such that $m \neq 4$ and let $g(y)$ be an irreducible polynomial in $Q[y]$. Then there are only finitely many rational solutions $(x,\ y)$ with bounded denominator of the equation* $x(x+1)(x+2)\cdots(x+m-1) = g(y)$.
- *When $m = 4$ and $g(y)$ be an irreducible polynomial in $Q[y]$ then equation $x(x+1)(x+2)\cdots(x+m-1) = g(y)$ has infinitely many solutions only when $g(y) = \frac{9}{16} + b\delta(y)^2$ where $b \in Q^*$ and $\delta(y) \in Q[y]$ is a linear polynomial. Besides this, the above equation has only finitely many solutions.*

More interesting part: we were able to bound $m$, the degree of $f$ whenever $g(y)$ is an irreducible polynomial.

### Theorem

*Assume that $g(y)$ is an irreducible polynomial in $Q[y]$ and $\Delta$ be a positive integer. Then there exists a constant $C = C(\Delta, g)$ such that for any $m \geq C$, the equation $x(x+1)(x+2)\cdots(x+m-1) = g(y)$ does not have any rational solution with bounded denominator $\Delta$. Moreover, $C$ can be calculated effectively.*

# Idea of the Proof

Idea : if you take product of any $d$ consecutive integers then that product is definitely divisible by $d$.

- 8.9.10.11 is divisible by 4
- 35.36.37.38.39.40.41 is divisible by 7

# Idea of the Proof

- for any prime $P$, when $m \geq P$ , $x(x+1)(x+2)\cdots(x+m-1)$ is divisible by $P$.

  In other words, polynomial $x(x+1)(x+2)\cdots(x+m-1)$ has root modulo $P$ for every $P$.

- Since $g(y)$ is an irreducible polynomial, there are infinitely many primes $P$ such that $g(y)$ does not have root modulo $P$.

- Choose smallest and **suitable** prime $P$ such that $g(y)$ does not have root modulo $P$. Then one can prove that for $m \geq P$, $f(x) = g(y)$ does not have root modulo $P$.

- $C = P$ will be the bound for $m$.

# Diophantine Equation Reduced to Elliptic Curve

- $r + s + t = rst = 1$ where $r,\ s,\ t$ are algebraic integers in the ring of the integers of quadratic field.

**Theorem (With K. Chakraborty(Acta Arithmetica))**

*If $K = Q(\sqrt{d})$ is a quadratic field with $d$ a square free integer, then except for $d = -1$ and $2$, the equation $r + s + t = rst = 1$ has no solution in the ring of integers of $K$.*

# Diophantine Equation Reduced to Elliptic Curve

- $r + s + t = rst = 1$

– Used theory of elliptic curves to get the result.

– From the Diophantine equation, by doing the change of variable, one gets the elliptic curve $y^2 = x^3 + 621x + 9774$. The result is proved by looking at the rational points on the elliptic curve.

# Outline

- Introduction
- Diophantine equations of the type $f(x) = g(y)$
- **Current Research in Diophantine Equations**

# Current Research in Diophantine Equations

T. N. Venkatramana (TIFR) in his paper( Proc.Int.Con.-Number Theory, No 1, 2004, pp. 155-161) has proved the following:

Let $a$ and $b$ be coprime positive integers and for an integer $n \neq 0$, let $\phi(n)$ be the number of positive integers not exceeding $|n|$ and coprime to $n$. Consider the infinite sequence $\phi(ax+b); x = ..... -2, -1, 0, 1, 2, 3.....$ and let $g(a, b)$ denote the $gcd$ of the numbers occurring in the above sequence. Then $g(a, b)$ is bounded by 4 for all $a$ and $b$.

We are trying to prove it for quadratic polynomials.

- We have $f(x) = ax^2 + bX + c$ where $a, b, c \geq 0$,

– look at $f(0),\ \ f(1),\ \ f(2),\ \ f(3), \ldots .f(-1),\ \ f(-2), \ldots ..$

– calculate $\phi f(0),\ \phi f(1),\ \phi f(2),\ \ldots\phi f(-1),\ \phi f(-2), \ldots ..$

– find the gcd of numbers occurring in the above sequence.

- for any prime $m \geq 5$, there exist a residue $r$ mod $m$ such that $f(r) \neq 0$ or 1 mod $m$.

– get $s = mx + r$ such that

$f(s) = f(mx + r) = p$ for some prime $p$

– Is it true that for some $n \in Z$,

$a(mn + r)^2 + b(mn + r) + c = p$ for some prime $p$.

**Observations:**

- $b$- even, monic polynomial $f(x) = x^2 + bx + c$, takes values $n+1,\ n+4,\ n+9,\ n+16, ..., n+d^2$, for fixed $n$.

- for some $d \in Z$, $n + d^2 \stackrel{?}{=} p$

- $b$ - odd, monic polynomial $f(x) = x^2 + bx + c$, takes values $n+2,\ n+6,\ n+12, ..., n+d+d^2$, for fixed $n$.

- for some $d \in Z$, $n + d + d^2 \stackrel{?}{=} p$