Reducing Complicated Objects to Simple Ones:
Coefficients of Modular Forms

Robert C. Rhoades
University of Wisconsin - Madison

September 27, 2005
Why work with complicated objects at all?

To solve problems!

★ Some problems are hard!
★ To understand what is going on we must work with complicated objects.

A Hard Problem:

Fermat’s Last Theorem

Are there integers $X, Y, Z$ so that

$$X^n + Y^n = Z^n?$$

This is a natural question because of the $n = 2$ case.

★ This problem went unsolved for over 300 years! To solve this problem we study “complicated objects”, in particular Modular Forms.
Background:
Modular Arithmetic

We say that \( m \equiv r \pmod{p} \), read \( m \) is congruent to \( r \) modulo \( p \), if \( r \) is the remainder of \( m \) when we divide \( m \) by \( p \).

**Example**  Let \( p = 7 \) Then we have the following

1. \( 13 \equiv 6 \pmod{7} \)
2. \( 21 \equiv 0 \pmod{7} \)

**Example**  Let \( p = 5 \) Then we have the following

1. \( 23 \equiv 3 \pmod{5} \)
2. \( 11000101 \equiv 1 \pmod{5} \)
• We can **add** and **multiply** using the name rules as before.

1.

\[
13 + 7 \equiv 20 \equiv 0 \pmod{5} \\
13 + 7 \equiv 3 + 2 \equiv 5 \equiv 0 \pmod{5}
\]

2.

\[
13 \times 7 \equiv 91 \equiv 1 \pmod{5} \\
13 \times 7 \equiv 3 \times 2 \equiv 6 \equiv 1 \pmod{5}
\]

This is sometimes called *clock arithmetic* since our clock works modulo 12.

**Example**  If it is 1 o’clock then 13 hours later it is 2 o’clock since \(1 + 13 \equiv 14 \equiv 2 \pmod{12}\).
A Simple Object

Binomial Coefficients

Begin with \((x+1)\) and raise it to the \(n\)th power. Multiplying out we get a new polynomial.

\[
(x + 1)^2 = x^2 + 2x + 1 \\
(x + 1)^3 = x^3 + 3x^2 + 3x + 1 \\
(x + 1)^4 = x^4 + 4x^3 + 6x^2 + 4x + 1 \\
\text{etc...}
\]

We can write

\[
(x+1)^n = \binom{n}{n}x^n + \cdots + \binom{n}{j}x^j + \cdots + \binom{n}{1}x^1 + \binom{n}{0}.
\]
Question:
What are its coefficients?

Properties of $\binom{n}{k}$.

1. $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$

2. $\binom{n}{k} = \binom{n}{n-k}$

3. $\binom{n}{0} = 1$ and $\binom{n}{1} = n$.

4. We have an exact formula!!

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Start with a basic object $(x + 1)$, do a natural operation of raising it to powers, and ask what the object looks like now.
A Slightly More Complicated Object:  
Elliptic Curves

An elliptic curve is

$$E : y^2 = x^3 + Ax + B.$$  

**Question:**
What are \((x, y)\) that satisfy the equation? How many solutions are there?

**Answer:** If \(x, y \in \mathbb{R}\) we can graph the equation.

If \(x, y \in \mathbb{Q}\) we can’t draw a picture as easily. But our picture would be a bunch of dots on the graph we drew in \(\mathbb{R}\).

**Question:**
What are \((x, y)\) modulo \(p\) that satisfy \(E\)?
An Example:

\[ E : y^2 = x^3 + 1 \]

To find the solutions we can just try all the different possibilities.

* Let \( p = 3 \) The solutions are \((x, y) = (0, 1),\)
  \((0, 2), (2, 0)\). So there are 3 solutions.

* Let \( p = 5 \) The solutions are \((x, y) = (0, 1),\)
  \((0, 4), (2, 2), (2, 3), (4, 0)\). So there are 5 solutions.

* Let \( p = 7 \). The solutions are \((x, y) = (0, 1), (0, 6),\)
  \((1, 3), (1, 4), (2, 3), (2, 4), (3, 0), (4, 3), (4, 4),\)
  \((5, 0), (6, 0)\). So there are 11 solutions.
**Definition** Let $N(p)$ be the number of solutions modulo $p$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N(p)$</td>
<td>3</td>
<td>5</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>17</td>
<td>9</td>
<td>23</td>
<td>29</td>
<td>11</td>
</tr>
</tbody>
</table>

**Question:**
What is $N(p)$?
A Complicated Object: Modular Forms

1. Complex Valued function $f : \mathbb{C} \to \mathbb{C}$.

2. Satisfies “nice” transformation laws. It is periodic

\[ f(z) = f(z + 1). \]

And satisfies

\[ f \left( \frac{1}{z} \right) = \pm f(z), \]

where $\pm$ depends on $f$ not on $z$.

3. Has a Fourier expansion so we can write it as

\[ f(z) = a(0) + a(1)q + a(2)q^2 + a(3)q^3 + \ldots, \]

where $q := e^{2\pi iz}$. The numbers $a(n)$ are called the coefficients of the modular form.
It may seem like these requirements are a lot to ask for. So are there any Modular forms at all?

**An Example**

\[ f(z) : = f(q) = q \prod_{n=1}^{\infty} (1 - q^{6n})^4. \]

**WHY?** To see that \( f(z + 1) = f(z) \) we use that \( e^{2\pi i} = 1 \) and \( e^{2\pi i(z+1)} = e^{2\pi i} e^{2\pi i z} = q \). Then it follows easily that \( f(z + 1) = f(z) \).

Also,

\[
\begin{align*}
\sum_{n=1}^{\infty} c(n)q^n &= q - 4q^7 + 2q^{13} + 10q^{19} - 21q^{25} + 20q^{31} + \cdots
\end{align*}
\]
Our Question

What are the coefficients of the modular form?

Why do we care?

If we understand the coefficients then we know everything about the modular form!
Why Study Modular Forms?

- They can give us information about number theoretic objects
  - partition numbers: the number of ways of representing numbers as the sum of smaller numbers
  - the number of ways of writing a number as the sum of squares, cubes, 4th powers

- They can give us information about the analytic continuation of important functions like the Riemann $\zeta$-function.

- They help us study our problem of determining $N(p)$. 
Theorem: [The Modularity of Elliptic Curves]
For every elliptic curve there is a modular form with coefficients \( c(p) \) such that

\[
N(p) + c(p) = p
\]
for all primes \( p \). Equivalently, \( N(p) = p - c(p) \).

- If we want to solve our problem about Elliptic Curves we just study modular forms!

★ This is a very difficult very important theorem. It was proved by Wiles, Taylor, Diamond and others.
• In our example $E : y^2 = x^3 + 1$ and the corresponding modular form is

$$f(q) = q \prod_{n \geq 1} (1 - q^{6n})^4.$$
The Beautiful Relationship

Theorem: [RL]

\[ c(p) \equiv \begin{cases} \frac{5(p-1)}{p-1} \mod 6 & \text{if } p \equiv 1 \pmod{6} \mod p \\ 0 & \text{if } p \not\equiv 1 \pmod{6} \end{cases} \] (1)

★ So the binomial coefficient are the same as the coefficients of a modular form!

How do we prove this?
1. Modular Forms $\Rightarrow$ Elliptic Curves
   - Modularity of Elliptic Curves

2. Elliptic Curves $\Rightarrow$ Finite Character Sums

3. Finite character sums $\Rightarrow$ Gamma Function (a generalization of the factorial function)
   - Gauss Sums
   - The celebrated Gross-Koblitz formula

4. Gamma Function $\Rightarrow$ Binomial Coefficients
   - Taylor Series
   - Modular Arithmetic
Conclusion

Beginning with a complicated object we continually reduce the object to a less complicated object until we are left with an object that we understand.

Thanks:

- Po-Ru Loh (Caltech)
- Jeremy Rouse (UW - Madison)
- Ken Ono (UW - Madison)