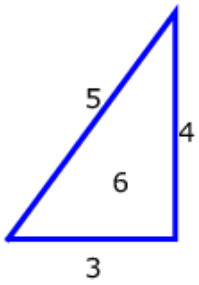
The Congruent Number Problem: A Thousand Year Old Unsolved Problem

William Stein (`http://modular.math.washington.edu`)

SIMUW 2006

Abstract

One of the oldest unsolved problems in mathematics is to determine the *congruent numbers*: *Give a way to decide whether or not an integer is the area of a right triangle with rational side lengths.* For example, 6 is the area of the right triangle with side lengths 3, 4, and 5. But 1 is not a congruent number. What about 2006? This workshop will take us from ancient [illegible] at has a milli[illegible]e.



The first few congruent numbers: 5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47, 52, 53, 54, 55, 56, 60, 61, 62, 63, 65, 69, 70, 71, 77, 78, 79, 80, 84, 85, 86, 87, 88, 92, 93, 94, 95, 96, 101, 102, 103, 109, 110, 111, 112, 116, 117, 118, 119, 120, 124, 125, 126, 127, 133, 134, 135, 136, 137, 138, 141, 142, 143, 145, 148, 149, 150, 151, 152, 154, 156, 157, 158, 159, 161, 164, 165, 166, 167, 173, 174, 175, 180, 181, 182, 183, 184, 188, 189, 190, 191, 194, 197, 198, 199, 205, 206, 207, 208, 210, 212, 213, 214, 215, 216, 219, 220, 221, 222, 223, 224, 226, 229, 230, 231, 237, 238, 239, 240, 244, 245, 246, 247, 248, 252, 253, 254, 255, 257, 260, 261, 262, 263, 265, 269, 270, 271, 276, 277, 278, 279, 280, 284, 285, 286, 287, 291, 293, 294, 295, 299, 301, 302, 303, 306, 308, 309, 310, 311, 312, 313, 316, 317, 318, 319, 320, 323, 325, 326, 327, 330, 333, 334, 335, 336, 340, 341, 342, 343, 344, 348, 349, 350, 351, 352, 353, 357, 358, 359, 365, 366, 367, 368, 369, 371, 372, 373, 374, 375, 376, 380, 381, 382, 383, 384, 386, 389, 390, 391, 395, 397, 398, 399, 404, 405, 406, 407, 408, 410, 412, 413, 414, 415, 421, 422, 423, 426, 429, 430, 431, 434, 436, 437, 438, 439, 440, 442, 444, 445, 446, 447, 448, 453, 454, 455, 457, 461, 462, 463, 464, 465, 468, 469, 470, 471, 472, 476, 477, 478, 479, 480, 485, 486, 487, 493, 494, 495, 496, . . . , 1974, 1975, 1976, 1980, 1981, 1982, 1983, 1984, 1989, 1990, 1991, 1995, 1997, 1998, 1999, 2000, 2004, 2005, 2006, 2007, 2008, 2009,. . .

Contents

Goals:

- Learn about a major open problem in number theory.
- Learn to use SAGE to draw plots and do computations.
- Learn about elliptic curves: groups, public-key cryptography, the BSD conjecture.

1 Rational Right Triangles

1. Statement of the congruent number problem.
2. Explain what "enumerate means".
3. Explain how to enumerate all right triangles with integer side lengths – Pythagorean triples: draw graph of circle; draw line; find other point of intersection; write it as (x, y) with x, y in terms of t.
4. SAGE tutorial:
   (a) What is SAGE?
   (b) SAGE website.
   (c) SAGE notebook: everyone create a worksheet.

- COMPUTATION:
  - Computer lab orientation.
  - Introduction to SAGE .
  - Write a program to enumerate rational numbers (make table).
  - Write a program to enumerate Pythagorean triples (make table).
  - Write a program that enumerates rational right triangles (make table).
  - Write a program that enumerates congruent numbers (make table).
  - Draw plots of numerous rational right triangles (use the `polygon` command in SAGE).
- THEORY:
  - Give a way to enumerate all rational numbers.
  - Give a way to enumerate all rational right triangles.
  - Prove that n is a congruent number if and only if nk^2 is a congruent number for any positive integer k.
  - Give a way to enumerate all congruent numbers. I.e., a procedure that outputs only congruent numbers and will eventually output any given congruent number.

- Give an explicit parametrization of all rational solutions (x, y) to the equation $5x^2 - y^2 = 4$.
- Give an example of an equation $ax^2 + by^2 = 1$ with $a, b \in \mathbb{Q}$ and $a, b > 0$ that has no rational solutions (x, y).

- RESEARCH:
  - Generalize the enumeration method from above to a method to find all rational solutions to any equation $ax^2 + by^2 = c$, when you're given one solution $P = (x, y)$.
  - Use the internet to try to figure out what the "local-to-global principle for binary quadratic forms" is. Give examples that illustrate it.
  - **Open problem:** Consider an equation $y^2 = f(x)$ with f a polynomial of degree 5. It is a very deep theorem (of Fields Medalist Gerd Faltings) that there are only finitely many rational solutions $(x, y) \in \mathbb{Q}^2$ of $y^2 = f(x)$. It is an open problem to give an algorithm that takes as input f and outputs all the solutions to $y^2 = f(x)$. This is currently a very active area of research.

2 Congruent Numbers and Elliptic Curves

Today's workshop is about the connection between congruent numbers and elliptic curves.

1. Daily crashing of the SAGE Notebook.
2. The Simuw SAGE Notebooks: login/password, graphics, tab completion, using mathematica/maple/etc from it.
3. Why are they called "congruent numbers"? Connection between congruent numbers and "congruences" modulo n.
4. 10-minute break.
5. Definition of elliptic curve.
6. Connection between congruent numbers and elliptic curves.

- COMPUTATION:
  - Find the point on an elliptic curve corresponding to the $(3, 4, 5)$-triangle.
  - Find the point on an elliptic curve corresponding to a rational right triangle with area 2006.
  - Download a table from workshop website of the congruent numbers up to 1000, and look for patterns, e.g., reduce the congruent numbers modulo 8, etc., and see if you notice anything.

- Find a rational number x such that $x-6, x, x+6$ are all perfect squares.
- Find a rational number x such that $x-2006, x, x+2006$ are all perfect squares.
- Let n be the year you were born. Is it possible to find a rational number x such that $x-n, x, x+n$ are all perfect squares?

- THEORY:
  - Prove that if n is a congruent number then there exists a rational number x such that $x-n$, x, and $x+n$ are all perfect squares of rational numbers.

    [[Hint: Let $X < Y < Z$ be sides of a rational right triangle with area n. Let $x = (Z/2)^2$.]]
  - Suppose n is an integer and there exists a rational number x such that $n-x$, n, and $n+x$ are all perfect squares. Prove that n is a congruent number. [[Hint: from Koblitz's book (see page 4 of scan on website). Let $X = \sqrt{x+n} - \sqrt{x-n}$, $Y = \sqrt{x+n} + \sqrt{x-n}$, $Z = 2\sqrt{x}$. Then X, Y, Z are the sides of a right triangle and are all rational, and the triangle has area n.]]
  - Think about problems with a similar feel:
    1. Which integers are the area of a square with rational side lengths?
    2. Which integers are the perimeter of a square with rational side lengths?
    3. Which integers are the area of a rectangle with rational side lengths?
  - Let n be a rational number. Prove that there is a bijection between

$$A = \left\{ (a,b,c) \in \mathbb{Q}^3 \,:\, \frac{ab}{2} = n,\ a^2+b^2=c^2 \right\}$$

    and

$$B = \left\{ (x,y) \in \mathbb{Q}^2 \,:\, y^2 = x^3 - n^2 x, \text{ with } y \neq 0 \right\}$$

    given explicitly by the maps

$$f(a,b,c) = \left(-\frac{nb}{a+c},\ \frac{2n^2}{a+c} \right)$$

    and

$$g(x,y) = \left(\frac{n^2-x^2}{y},\ -\frac{2xn}{y},\ \frac{n^2+x^2}{y} \right).$$

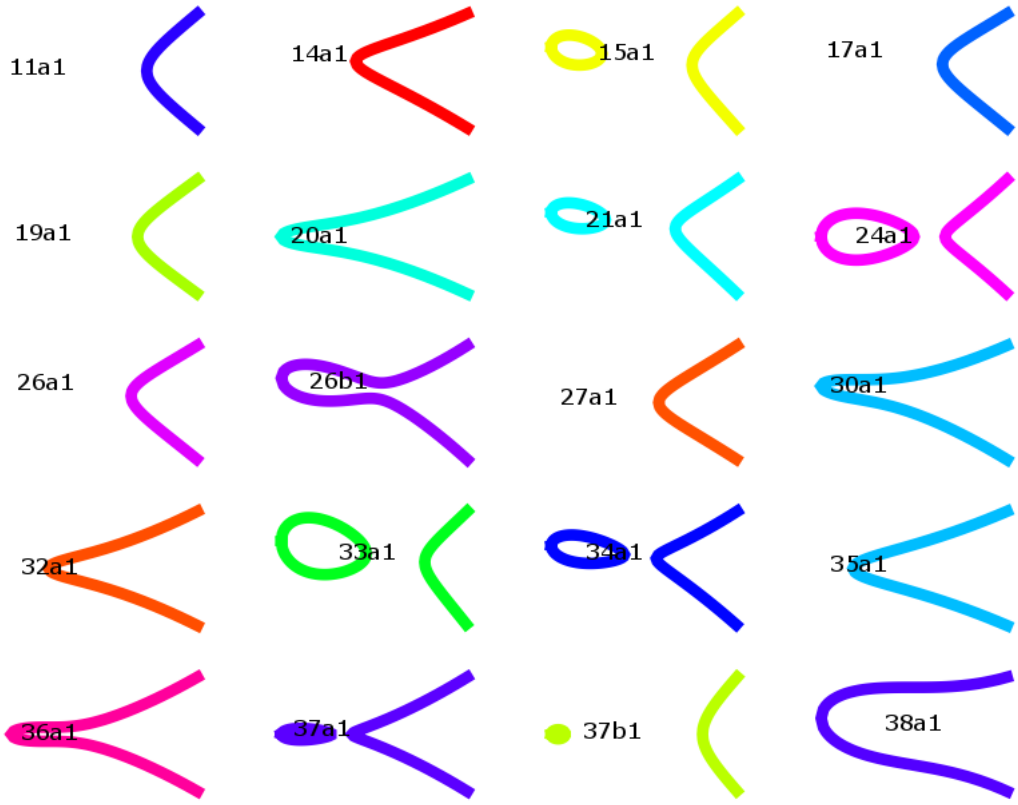
- RESEARCH:
  - Try to say something about which integers are the perimeter of a right triangle with rational side lengths. Try to convert this question to a question about solutions to equations.

– Be creative and come up with similar problems, e.g., which integers are the area of an equilateral triangle with rational side lengths, etc., some very hard, and convert each to a diophantine equation.

– Go to

  `http://www.msri.org/publications/ln/msri/2000/introant/yui/1/index.html`

  and read about another difficult generalization of the congruent number problem (this was a talk at a serious professional research conference, so don't be annoyed if you don't understand much of it).



For fun – the above are a bunch of elliptic curves, along with their **"Cremona labels"**.

3 Congruent Numbers and Elliptic Curves: II

1. **The Bijection Revisited Conceptually:** (75 minutes)

   (a) (2 minute) Definition of *congruent number*.

   (b) (2 minute) Definition of *elliptic curve*.

   (c) (40 minutes) *Bijection* between points and congruent triangles: revisited. In particular, here is a conceptual way to think about it. The set of rational right triangles with area n is the same as the set of simultaneous solutions to the system of equations

   $$a^2 + b^2 = c^2, \qquad \frac{ab}{2} = n.$$

   This is the intersection of two quadratic surfaces in 3-space, hence a curve. That curve turns out, after an appropriate change of variables, to be the elliptic curve $y^2 = x^3 - n^2 x$. Exercise: ...6 steps... (Solution presentation: 30 minute).

2. **Break:** (10 minute).

3. **Perimeter:** (15 minute) Discuss the problem of which integers are the perimeter of a right triangle with rational side lengths. Again, the set of such triangles for a given m is the set of simultaneous solutions to 2 equations:

   $$a^2 + b^2 = c^2, \qquad a + b + c = m.$$

   This is the intersection of a quadratic surface and a plane, hence a quadratic curve. (Exercise – 15 minutes trying this further; presentation of solution.)

4. **Generating New Points on Elliptic Curves from Other Points** (30 minutes): Explain how it works. Show how to use SAGE to do it. (Exercise – 30 minutes doing this (and getting new triangles); presentations.)

- COMPUTATION:

  – Find a triangle with perimeter 6. Hint: rescale the $3, 4, 5$ triangle. How does rescaling change the perimeter?

  – Find four distinct right triangles with area 6.

  – Let E be the elliptic curve defined by $y^2 = x^3 - 36x$, and let $P =$ Compute $P, 2P, 3P, 4P$ by enter E and P into SAGE and compute the given sums. Trying computing lots of other points too.

  ```
  sage: E = EllipticCurve([-36,0])
  sage: P = E([...])
  sage: 2*P
  ```

- THEORY:

– Fix an integer n. Show that the rational right triangles with area n are in bijection with the solutions to $y^2 = x^3 - n^2x$ with $y \neq 0$ as follows:

1. Think purely conceptually (don't write anything down!):
   (a) Imagine the surface
   $$a^2 + b^2 = c^2$$
   in three-dimensional space.
   (b) Next imagine the surface
   $$\frac{ab}{2} = n$$
   in three-dimensional space.
   (c) Finally, imagine the intersection of those two surfaces. You should be visualizing a curve in three dimensional space.
2. Solve for a in the equation $ab/2 = n$ and substitute it into $a^2 + b^2 = c^2$ to obtain an equation of the curve you visualized in three space in the previous problem. You should be able to put this curve in the form
   $$4n^2 + X^4 = Y^2.$$
   (You'll have to let X and Y equal something involving a and b.)
3. Replace X by y_1 and Y by $x_1 + y_1^2$ in the equation for your curve. Simplify and get another curve (but in the variables x_1 and y_1):
   $$4n^2 = x_1^2 + 2y_1^2x_1$$
   You should be able to do all this by hand. But if you want to use a computer, here's an example of how in SAGE:
   ```
   sage: X = gp('X'); Y = gp('Y'); x_1 = gp('x_1')
   sage: y_1 = gp('y_1'); n = gp('n')
   sage: print (Y^2).subst(Y,x_1+y_1^2).subst(X, y_1)
   sage: print (4*n^2 + X^4).subst(Y,x_1+y_1^2).subst(X, y_1)
   x_1^2 + 2*y_1^2*x_1 + y_1^4
   y_1^4 + 4*n^2
   ```
   (In SAGE the command `gp('stuff')` makes a formal variable, and `subst` allows you to do formal substitutions.)
4. Multiply both sides of the equation you obtain by x_1, then replace x_1 by x_2 and y_1 by y_2/x_2, to obtain:
   $$4n^2x_2 = x_2^3 + 2y_2^2.$$
5. Do a few additional manipulations to finally obtain the equation
   $$y^2 = x^3 - n^2x.$$

6. If you combine everything you've done so far you get a bijection from yesterday (you do not have to show this). Moreover, you can now go back and forth between solutions to $y^2 = x^3 - n^2x$ and rational right triangles with area n. For example, try this with $n = 6$.
   (a) Show that the point on the cubic $y^2 = x^3 - 36x$ that corresponds to the $3, 4, 5$ triangle is $(-3, 9)$.
   (b) Use SAGE to find another point Q on $y^2 = x^3 - 36x$.
   (c) Find the triangle corresponding to Q. Verify that it really does have area 6.

- RESEARCH:
  - Say something about perimeters of rational right triangles. Convert this question to a question about solutions to some equation (as bove). Solve this other equation. Give a systematic way to enumerate all rational right triangles with given perimeter.

4 Elliptic Curve Groups

1. (15 minutes) Presentation – Perimeters of right triangles? Patterns in congruent numbers modulo 8?

2. (30 minutes) Definition of a *group*.

   Definition 4.1. An **abelian group** is a set X equipped with a binary operation $+$ and an element $0 \in X$ such that for all $a, b, c \in X$,

   (a) (closure) $a + b \in X$,

   (b) (identity) $0 + a = a + 0 = a$,

   (c) (associativity) $a + (b + c) = (a + b) + c$,

   (d) (inverses) for every a in X there is d such that $a + d = 0$,

   (e) (commutativity) $a + b = b + a$.

   Examples:

   (a) The **integers** $\mathbb{Z} = \{0, -1, 1, -2, 2, -3, 3, \ldots\}$ under addition.

   (b) The **rational numbers** $\mathbb{Q}$ under addition.

   (c) The **integers** $\{0, 1, \ldots, n-1\}$ under **addition modulo** n.

   (d) Let p be a prime. The **integers** $\{1, \ldots, p-1\}$ under **multiplication modulo** p. This is called $\mathbb{F}_p^*$.

3. (15 minutes) Experiment with some abelian groups in SAGE .

4. (10 minutes) Break.

5. (20 minutes) Definition of elliptic curve groups.

   Definition 4.2. Fix integers a and b. Let $E(\mathbb{Q})$ be the set of solutions to $y^2 = x^3 + ax + b$ along with one "extra point" which we call $\mathcal{O}$ which is the additive 0 element. This is an abelian group (note: the associative law takes a *lot* of work to prove!).

6. (30 minutes) Participants: Graph elliptic curves. Then **derive an algebraic formula** (by hand) for the group operation.

7. (15 minutes) Elliptic curves modulo p. Fix integers a and b and a prime p. Let $E(\mathbb{F}_p)$ be the set of solutions to $y^2 \equiv x^3 + ax + b \pmod{p}$ with $0 \leq x < p$ and $0 \leq y < p$ along with a formal extra point $\mathcal{O}$. This group is central in both cryptography (in making *and* cracking cryptosystems) and the Birch and Swinnerton-Dyer conjecture! I will explain how in both cases next week.

8. (15 minutes) Participants: Graph and compute with some elliptic curves modulo p.

4.1 Elliptic Curves over $\mathbb{Q}$

- COMPUTATION:
  - Play around with each of the above groups in SAGE . Here are examples of how to compute with each of the groups listed above in SAGE to get you started. Be creative and experiment!

```
sage: ZZ
Integer Ring
sage: a = ZZ(5); b = ZZ(7); a+b
12

sage: QQ
Rational Field
sage: QQ(3/4) + QQ(2/3)
17/12

sage: R = IntegerModRing(12)
sage: print R
Ring of integers modulo 12
sage: R(7) + R(8)
3

sage: R = FiniteField(7)
sage: print R
Finite Field of size 7
sage: R(4)*R(5)
6
```

  - Compute with elliptic curves over $\mathbb{Q}$. Here is an example to get you started.

```
sage: E = EllipticCurve([-36,0])
sage: E
Elliptic Curve defined by y^2  = x^3 - 36*x over Rational Field
sage: P = E([-3,9])   # or use E.gens(proof=False)
sage: P + P
(25/4 : -35/8 : 1)
```

  - Draw some graphs of elliptic curves (using the new program I just wrote!). Here is an example to get you started:

```
sage: E = EllipticCurve([-36,0])
sage: P = plot(E,rgbcolor=(0,0,1))
sage: pnt = E([-3,9])
sage: pnt2 = 2*pnt
sage: c1 = point(pnt, pointsize=100)
sage: c2 = point(pnt2, rgbcolor=(1,0,0), pointsize=100)
sage: show(P + c1 + c2)
```

- THEORY:
  - Let E be an elliptic curve given by an equation $y^2 = x^3 + ax + b$. Prove that the following steps can be used to compute $+$ on E: Given P_1, P_2, this algorithm computes the third point $R = P_1 + P_2$.
    1. [Is $P_i = \mathcal{O}$?] If $P_1 = \mathcal{O}$ set $R = P_2$ or if $P_2 = \mathcal{O}$ set $R = P_1$ and terminate. Otherwise write $(x_i, y_i) = P_i$.
    2. [Negatives] If $x_1 = x_2$ and $y_1 = -y_2$, set $R = \mathcal{O}$ and terminate.
    3. [Compute λ] Set $\lambda = \begin{cases} (3x_1^2 + a)/(2y_1) & \text{if } P_1 = P_2, \\ (y_1 - y_2)/(x_1 - x_2) & \text{otherwise.} \end{cases}$
    4. [Compute Sum] Then $R = \big(\lambda^2 - x_1 - x_2, -\lambda x_3 - \nu\big)$, where $\nu = y_1 - \lambda x_1$ and $x_3 = \lambda^2 - x_1 - x_2$ is the x-coordinate of R.
- RESEARCH:
  - Using the Internet find two web pages that define abelian groups. Understand the definitions (perhaps by copying them down onto a piece of paper). Do they agree with the definition that I gave above?

4.2 Elliptic Curves Modulo p

Definition, arithmetic, point enumeration, elliptic curve cryptography (discrete log problem; diffie-hellman).

- COMPUTATION:
  - Compute with elliptic curves modulo a prime p. Here is an example to get you started.

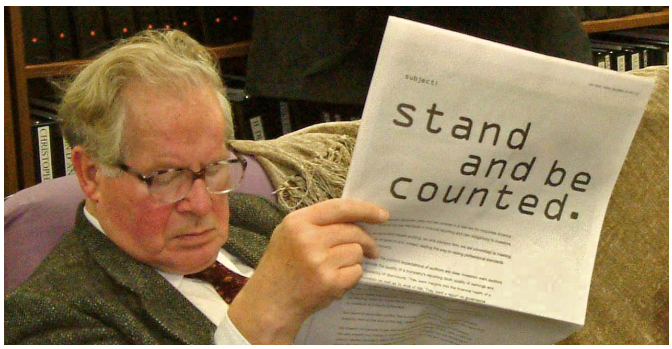
```
sage: E = EllipticCurve(FiniteField(43), [-36,0])
sage: E
Elliptic Curve defined by y^2  = x^3 + 7*x over Finite Field of size 43
sage: P = E([-3,9])
sage: P + P
(17 : 1 : 1)
```

  - Graph some elliptic curves modulo p:

```
sage: E = EllipticCurve(FiniteField(13), [-36,0])
sage: P = plot(E,rgbcolor=(0,0,1),pointsize=100)
sage: P.show(dpi=200)
```

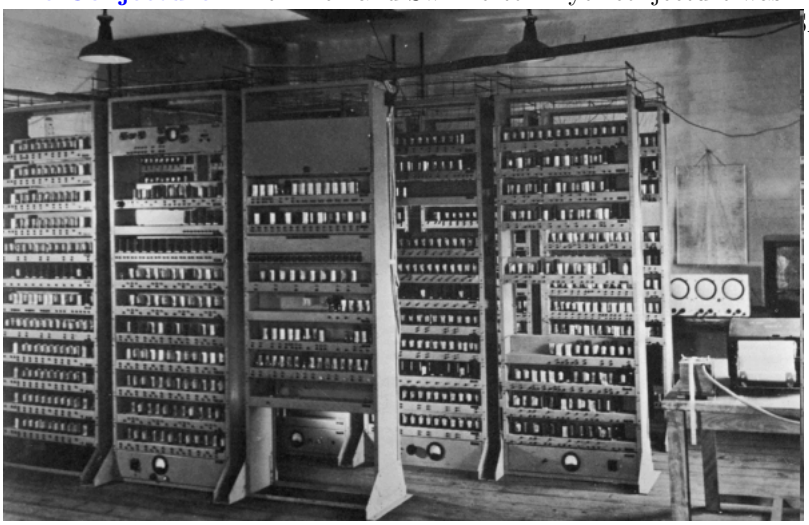
- THEORY:
  - Given P and a positive integer n, it is fairly straightforward to compute $nP = P + P + \cdots + P$. Given P and Q where you know that $Q = nP$ for some n (even though you don't know n!), invent a way to find n (it doesn't have to be fast).

5 The Birch and Swinnerton-Dyer Conjecture (Monday)



1. (15 minutes) Congruent number problem; connected to elliptic curves; we need to understand when elliptic curves have points on them.

2. (15 minutes) Daily crashing of the SAGE Notebook – some improvements I made over the weekend: computing `E.points()` for E an elliptic curve modulo p is now very fast; the Notebook interface is generally more robust and much easier to interrupt; `foo??` gives source code even for functions you enter or in cong.sage if you do `attach cong.sage`; can write, e.g., `plot(..., hue=...)` instead of `plot(..., rgbcolor=hue(...))`. So please, right now, try hard to "crash" your personal SAGE Notebook, i.e., get it in an unresponsive state. Don't worry, I can easily restart all of them.

3. **The Conjecture**. The Birch and Swinnerton-Dyer conjecture was made

AC:

Let n be a positive square-free integer. This means that no perfect square divides n. Let E_n be the elliptic curve

$$E_n: \quad y^2 = x^3 - n^2 x.$$

If n is odd, let $N = 32n^2$, and if n is even, let $N = 16n^2$. The number N is called the *conductor of E_n*.

For any prime $p \nmid 2n$, let

$$a_p = p + 1 - \#E_n(\mathbb{F}_p),$$

where $\#E_n(\mathbb{F}_p)$ is the number of points on the elliptic curve E_n viewed modulo p. If $p \mid 2n$, let $a_p = 0$. If m, r are coprime integers, let $a_{mr} = a_m a_r$. If $p \nmid 2n$ let $a_{p^r} = a_{p^{r-1}} a_p - p a_{p^{r-2}}$, and if $p \mid 2n$ let $a_{p^r} = 0$. Finally, let

$$L(E_n, 1) = \begin{cases} 0 & \text{if } n \equiv 5, 6, 7 \pmod 8 \\ 2 \cdot \sum_{k=1}^{\infty} \frac{a_k}{k} \cdot e^{-2\pi k/\sqrt{N}} & \text{otherwise.} \end{cases}$$

Conjecture 5.1 (Birch and Swinnerton-Dyer)**.**

We have $L(E_n, 1) = 0$ if and only if $E_n(\mathbb{Q})$ is infinite.

(Stated in a special cases.)

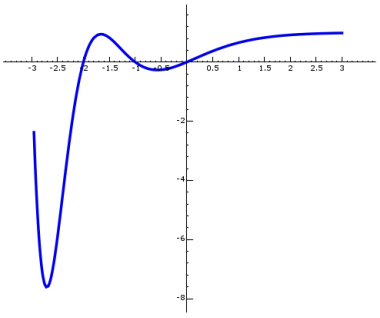
This is a *major open problem* in number theory. *If I don't solve this problem, I hope one of you does!*

Heuristic "Proof". (This is a **fake** "proof".) If $E_n(\mathbb{Q})$ is infinite then the numbers $\#E_n(\mathbb{F}_p)$ will tend to be *big*, since you get lots of elements of $E_n(\mathbb{F}_p)$ by reducing the elements of $E_n(\mathbb{Q})$ modulo p. Thus $a_p = p + 1 - \#E_n(\mathbb{F}_p)$ will tend to be *small*. One can prove that $L(E_n, 1) \geq 0$, so if the a_p are small, that will "cause" the sum that defines $L(E_n, 1)$ to be small, i.e., 0. Conversely if $L(E_n, 1) = 0$, then the $E_n(\mathbb{F}_p)$ are big, and the points have to come from somewhere so $E_n(\mathbb{Q})$ is big. □

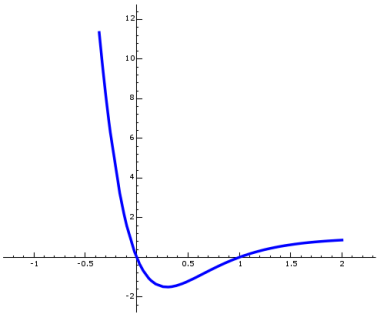
Theorem 5.2 (Kolyvagin et al.)**.** *If $E_n(\mathbb{Q})$ is infinite then $L(E_n, 1) = 0$.*

This is one direction in the conjecture, and the proof is *very very difficult*. Put another way, this theorem says that if $L(E_n, 1) \neq 0$, then $E_n(\mathbb{Q})$ is finite.

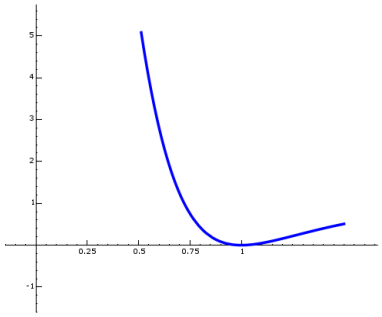
As the notation suggests, $L(E_n, 1)$ is the value of a function at 1. I will not define the general function, but here are some plots of $L(E_n, s)$ for various n:



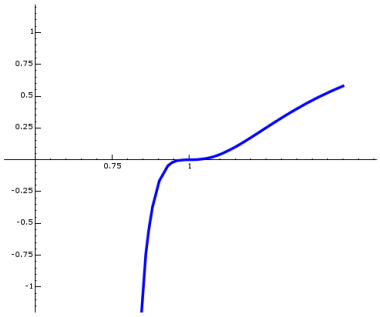
$n = 1$



$n = 6$



$n = 34$



$n = 4199$

I made them using code like

```
E = EllipticCurve([-6^2,0])
L = E.Lseries_dokchitser()
P = plot(L,0.5,1.5, plot_points=50, plot_division=50,
        rgbcolor=(0,0,1), thickness=2)
```

4. Participants – do the following for $n = 1$ and $n = 34$:

   (a) Write down E_n.

   (b) Find the conductor N of E_n.

   (c) Compute (by hand/with computer) a_1, a_2, a_3, a_4, and a_5. Check your answer with SAGE (use `E.an(m)` to compute a_m). The point here is to spend some time understanding the definition of a_m.

   (d) Compute the first 5 terms in the sum that defines $L(E_n, 1)$. (You should find that for $n = 34$ we have $L(E_{34}, 1) = 0$, whereas for $n = 1$ we have $L(E_1, 1) \neq 0$.)

```
sage: E = EllipticCurve([-1^2,0])
sage: E.Lseries(1)
```

```
0.65551438857302990

sage: E = EllipticCurve([-34^2,0])
sage: E.Lseries(1)
-0.0000000000000000...  (the nonzeros at the end are just errors/noise)
```

(e) The following SAGE program can be used to compute the sum that defines $L(E_n, 1)$ using any number of terms.

```
def L(n, prec):
   E = EllipticCurve([-n^2,0])
   v = E.anlist(prec)
   N = E.conductor()
   sqrtN = sqrt(N)
   lval = 2*sum(v[n]/n*exp(-2*pi*n/sqrtN) for n in range(1,prec))
   return lval
```

Note: This function is in `cong.sage`. Just type `attach cong.sage` if you haven't already and it will magically be available. Then you can enter `L?` for help and `L??` for source code.

5. Participants – Prove using SAGE calculations and the BSD conjecture that none of $1, 2, 3, 4$ are congruent numbers.

6. Participants – Try to find patterns, any at all, in the numbers

$$p + 1 - \#E_n(\mathbb{F}_p)$$

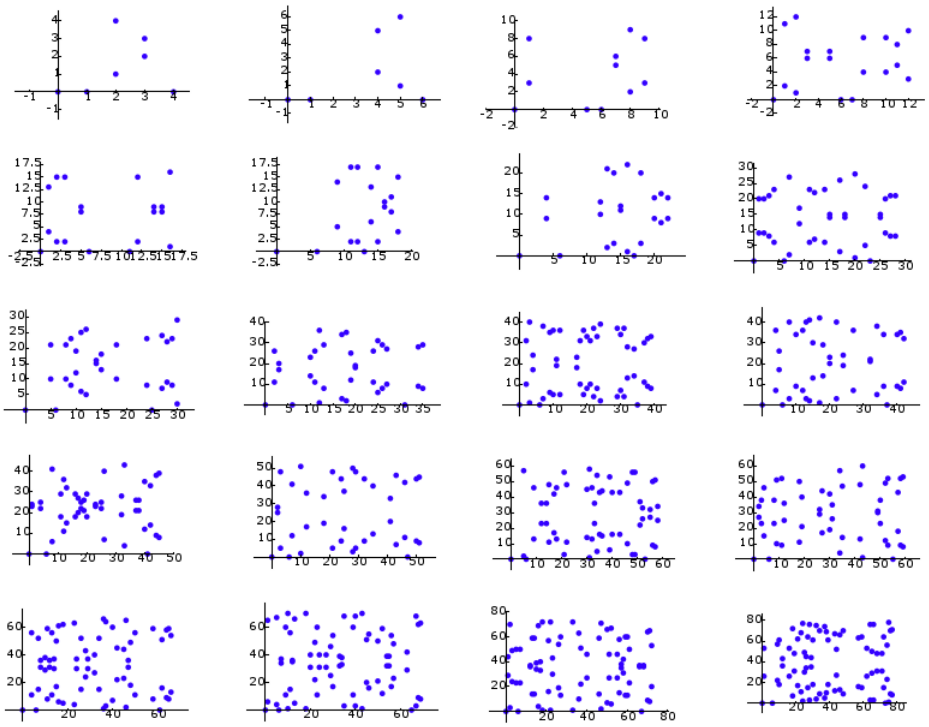
for the congruent number curves $y^2 = x^3 - n^2x$. E.g., fix $n = 1$ and compute these numbers for primes up to some bound:

```
E = EllipticCurve([-1,0])
for p in primes(2,100):
    print p, E.ap(p)
```

- COMPUTATION:
  - This SAGE code draws the plot below. Try different curves, ranges of primes, etc.

```
n = 6
def pl(p):
    return plot(EllipticCurve(GF(p),[-n^2,0]), rgbcolor=hue(0.7))

P = [pl(p) for p in primes(5,100) if n%p != 0]
Q = [[P[4*i+j] for j in range(4)] for i in range(len(P)/4)]
show(graphics_array(Q))
# show(graphics_array(Q), axes=False)   # if you don't want axes
```



  - Make a table of values $L(E_n, 1)$ for each integer $n < 50$. How does this compare to the table of congruent numbers $n < 50$. [Here's how to *approximately* compute $L(E, 1)$ in SAGE:]
  - In this problem n *always* denotes a squarefree positive integer n (i.e., no perfect squares divide n).
    1. If $n \equiv 5, 6, 7 \pmod 8$ then does the Birch and Swinnerton-Dyer conjecture imply that n is a congruent number?
    2. Are there *any* integers $n \equiv 3 \pmod 8$ with n a congruent number?

    `EllipticCurve([-1,0]).Lseries(1)`

- THEORY:
  - What is the relationship between the a_p for E_1 and E_6? Make a conjecture based on numerical evidence. Note: you can compute a_p using `E.ap(p)`, e.g.,

```
E = EllipticCurve([-1,0])
for p in primes(10):
    print p, E.ap(p)
```

Can you say anything about the relation between the a_p for E_1 and for E_n for general n?

- RESEARCH:
  - Find Andrew Wiles's paper on the Birch and Swinnerton-Dyer conjecture at the Clay Math Institute web site

    `http://www.claymath.org/millennium/`

    and read as much of it as you can. One of their pages says:

    > "Mathematicians have always been fascinated by the problem of describing all solutions in whole numbers x, y, z to algebraic equations like
    >
    > $$x^2 + y^2 = z^2.$$
    >
    > Euclid gave the complete solution for that equation, but for more complicated equations this becomes extremely difficult. Indeed, in 1970 Yu. V. Matiyasevich showed that Hilbert's tenth problem is unsolvable, i.e., there is no general method for determining when such equations have a solution in whole numbers. But in special cases one can hope to say something. When the solutions are the points of an abelian variety, the Birch and Swinnerton-Dyer conjecture asserts that the size of the group of rational points is related to the behavior of an associated zeta function $L(s)$ near the point $s = 1$. In particular *this amazing conjecture asserts that if $L(1)$ is equal to 0, then there are an infinite number of rational points (solutions), and conversely, if $L(1)$ is not equal to 0, then there is only a finite number of such points.*"

  - Noam Elkies web page

    `http://www.math.harvard.edu/~elkies/compnt.html`

    has the most extensive data I've seen about congruent numbers. Check it out!

  - EDSAC – search for information online about the EDSAC computer.

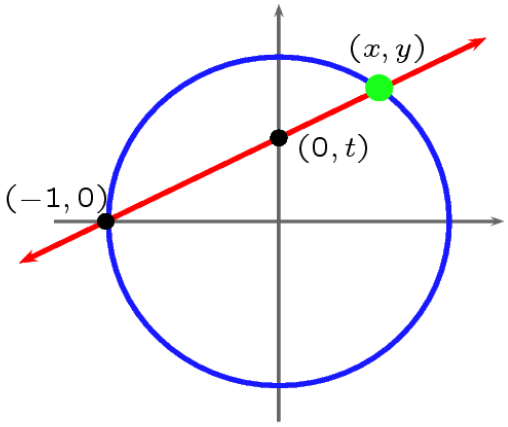
6 Square Triangles and Fermat's Last Theorem (Wed morning)

The numbers 1, 2, 3, and 4 are not congruent numbers. In particular, 1 is not. I.e., there is not rational right triangle whose area is a perfect square, i.e., there are no "square triangles".

1. (60 minutes) Watch the Fermat's Last Theorem movie.
2. (10 minutes) Move to computer lab / break.
3. (10 minutes) Recall that we "know" 1 is not a congruent number from Monday, since $L(E_1, 1) = 0.65551\ldots \neq 0$. But that uses a deep theorem (the proof by Kolyvagin of one direction of the Birch and Swinnerton-Dyer conjecture).
4. (70 minutes) Prove Fermat's Last Theorem for $n = 4$, and use this to deduce that 1 is not a congruent number.

- COMPUTATION:
  - Via a direct computer search, show there are no right triangles with area 1 and rational side lengths (a, b, c) (with c the hypotenuse) with the number of digits of the numerators and denominators of a, b, c all < 100 in absolute value.
  - Look for solutions to $y^2 = x^3 - x$ with both x, y rational and $y \neq 0$. Fail to find any.
- THEORY: You *definitely* want to work together on these problems, even possibly dividing up into groups and assigning parts to different groups, and also having people search online for help (which is allowed). Make solving all these nicely a community effort. [Credit: This sequence of problems was originally written by the Baur Bektemirov (the first ever winner of the International Math Olympiad gold medal from Kazakhstan), while he was a freshman at Harvard working with me.]
  1. Suppose a, b, c are relatively prime integers with $a^2 + b^2 = c^2$. Then there exist integers x and y with $x > y$ such that $c = x^2 + y^2$ and either $a = x^2 - y^2$, $b = 2xy$ or $a = 2xy$, $b = x^2 - y^2$. Hint: Recall what we did on day 1 where we parametrized Pythagorean triples a, b, c:

Enumerating Pythagorean Triples



$$\text{Slope} = t = \frac{y}{x+1}$$

$$x = \frac{1-t^2}{1+t^2}$$

$$y = \frac{2t}{1+t^2}$$

If $t = \frac{r}{s}$, then $a = s^2 - r^2, \quad b = 2rs, \quad c = s^2 + r^2$ is a Pythagorean triple, and all primitive unordered triples arise in this way. **We can solve two-variable quadratic equations.**

2. Fermat's Last Theorem for exponent 4 asserts that any solution to the equation $x^4 + y^4 = z^4$ with $x, y, z \in \mathbb{Z}$ satisfies $xyz = 0$. Prove Fermat's Last Theorem for exponent 4, as follows.
   (a) Show that if the equation $x^2 + y^4 = z^4$ has no integer solutions with $xyz \neq 0$, then Fermat's Last Theorem for exponent 4 is true. (Note – the power of x is 2.)
   (b) Prove that $x^2 + y^4 = z^4$ has no integer solutions with $xyz \neq 0$ as follows. Suppose $n^2 + k^4 = m^4$ is a solution with $m > 0$ minimal amongst all solutions. Show that there exists a solution with m smaller using the previous exercise above (consider two cases).
3. Prove that 1 is not a congruent number by showing that the cubic curve $y^2 = x^3 - x$ has no rational solutions except $(0, \pm 1)$ and $(0, 0)$:
   (a) Write $y = \frac{p}{q}$ and $x = \frac{r}{s}$, where p, q, r, s are all positive integers and $\gcd(p, q) = \gcd(r, s) = 1$. Prove that $s \mid q$, so $q = sk$ for some $k \in \mathbb{Z}$.
   (b) Prove that $s = k^2$, and substitute to see that $p^2 = r^3 - rk^4$.
   (c) Prove that r is a perfect square by supposing that there is a prime ℓ such that $\text{ord}_\ell(r)$ is odd and analyzing ord_ℓ of both sides of $p^2 = r^3 - rk^4$.
   (d) Write $r = m^2$, and substitute to see that $p^2 = m^6 - m^2k^4$. Prove that $m \mid p$.
   (e) Divide through by m^2 and deduce a contradiction to the previous exercise.

7 An Elementary Criterion (Thursday)

1. (< 1 hour) – Student presentations: proof of FLT for exponent 4 and no square triangles.

2. (10 minutes) – break

3. (30 minutes) – statement of Tunnell's criterion. Let

$$\Theta(q) = 1 + 2\sum_{m\geq 1} q^{m^2} = 1 + 2q + 2q^4 + 2q^9 + \cdots .$$

Let

$$f_1 = \Theta(q) \cdot (2\Theta(q^{32}) - \Theta(q^8)) \cdot \Theta(q^2)$$

and

$$f_2 = \Theta(q) \cdot (2\Theta(q^{32}) - \Theta(q^8)) \cdot \Theta(q^4).$$

Theorem 7.1 (Waldspurger, Tunnell)**.** *Suppose n is a squarefree integer. If n is odd then $L(E_n, 1) = 0$ if and only if the nth coefficient of f_1 is 0. If n is even then $L(E_n, 1) = 0$ if and only if the $\frac{n}{2}$th coefficient of f_2 is 0.*

This is a **very deep theorem**. It allows us to determine whether or not $L(E_n, 1) = 0$. The Birch and Swinnerton-Dyer conjecture (which is not a theorem) then asserts that $L(E_n, 1) = 0$ if and only if n is a congruent number. Thus once enough of the Birch and Swinnerton-Dyer conjecture is proved, we'll have an elementary way to decide whether or not a (squarefree) integer n is a congruent number. Namely, if n is odd then (conjecturally) n is a congruent number if and only if

$$\#\left\{x, y, z \in \mathbb{Z} : 2x^2 + y^2 + 32z^2 = n\right\} = \frac{1}{2}\#\left\{x, y, z \in \mathbb{Z} : 2x^2 + y^2 + 8z^2 = n\right\}.$$

Simiarly, if n is even then (conjecturally) n is a congruent number if and only if

$$\#\left\{x, y, z \in \mathbb{Z} : 4x^2 + y^2 + 32z^2 = \frac{n}{2}\right\} = \frac{1}{2}\#\left\{x, y, z \in \mathbb{Z} : 4x^2 + y^2 + 8z^2 = n\right\}.$$

4. (30 minutes) – exercises with Tunnell's criterion.

   (a) Come up with a method to explicitly list each of the above sets.

   (b) Prove that the elementary criterion (involving cardinality of sets) implies that none of $n = 1, 2, 3, 4$ are congruent numbers.

   (c) Prove that the elementary criterion (involving cardinality of sets) implies that $n = 5, 6, 7$ are congruent numbers. Then find a right triangle with area 5.

   (d) Verify with SAGE that Theorem 7.1 (appears to) hold for $n < 20$. Hint: The command

```
f1, f2 = tunnell_forms(30)
```

computes the f_1 and f_2 defined above, and e.g., `f1[3]` returns the coefficient of q^3.

(e) **Question (Nathan Ryan):** Is it possible to decide whether or not a prime number p is a (conjectural) congruent number in time polynomial in the number of digits of p? I.e., if p has a hundred digits is there any hope we could tell whether or not p is (conjecturally) a congruent number i a reasonable amount of time? [[**WARNING: This is an unsolved problem, as far as I know.**]]

8 Square Triangles Revisited

Since there was so much trouble with the proof of Fermat for exponent 4, let's revisit it. First, Fermat's proof:

> "if the area of a rational right triangle were a square, then there would also be a smaller one with the same property, and so on, which is impossible."

OK, that wasn't so helpful. Anyway, we did everything on Thursday except 2b, i.e., suppose that $n^2 + k^4 = m^4$ is a solution in positive integers to the equation $x^2 + y^4 = z^4$ with $m > 0$ minimal among all possible solutions. Show that there is a a smaller solution, hence deduce a contradiction.

1. Case 1: If n is even then there exist integers $x, y \geq 0$ (with $x > y$) such that
$$n = 2xy \qquad k^2 = x^2 - y^2 \qquad m^2 = x^2 + y^2.$$
Then
$$(mk)^2 = x^4 - y^4,$$
from which we obtain a smaller solution.

2. Case 2: Next assume n is odd. The trick is to proceed as above, but to apply exercise 1 again to the Pythagorean triple $m^2 = x^2 + y^2$ and note that various numbers are perfect squares. We give full details below.

   There are integers x, y with $x > y$ such that
$$n = x^2 - y^2 \qquad k^2 = 2xy \qquad m^2 = x^2 + y^2.$$
   Since $2xy = k^2$ is a perfect square we can write either $x = u^2$, $y = 2v^2$ or $x = 2u^2$, $y = v^2$ for integers u, v.

   (a) Case: We have $x = u^2, y = 2v^2$, i.e., y is even and x is odd (note that x must be odd if y is even since $n = x^2 - y^2$ is odd). Since $m^2 = x^2 + y^2$ is itself a Pythagorean triple with x odd, we can again apply exercise 1 to find coprime integers a, b such that
$$x = a^2 - b^2 \qquad y = 2ab \qquad z = a^2 + b^2.$$
   Then $2v^2 = y = 2ab$, so since a, b are coprime we have $a = d^2$, $b = e^2$ for integers d, e. Since $x = u^2$ and $x = a^2 - b^2$, we have
$$u^2 = d^4 - b^4,$$
   which yields a smaller solution to $x^2 + y^4 = z^4$.

(b) Case: We have $x = 2u^2, y = v^2$, i.e., y is odd and x is even (note that y must be odd if x is even since $n = x^2 - y^2$ is odd). Since $m^2 = x^2 + y^2$ is itself a Pythagorean triple with y odd, we can again apply exercise 1 to find coprime integers a, b such that

$$y = a^2 - b^2 \qquad x = 2ab \qquad z = a^2 + b^2.$$

Then $2u^2 = x = 2ab$, so since a, b are coprime and have square product we have $a = d^2$, $b = e^2$ for integers d, e. Since $y = v^2$ and $y = a^2 - b^2$, we have

$$v^2 = d^4 - b^4,$$

which yields a smaller solution to $x^2 + y^4 = z^4$.

9 An Elliptic Curve Cryptography (ECC) Tutorial

Elliptic curves are useful far beyond the fact that they shed a huge amount of light on the congruent number problem. For example, many people (probably you!) use them on a daily basis, since they are used to make some of the best public-key cryptosystems (= methods for sending secret data).

I think the Wikipedea opening description of Elliptic curve cryptography is OK (no comment about the rest of the article):

> Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz [1] and Victor S. Miller [2] in 1985.
>
> Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as, for instance, Lenstra elliptic curve factorization, but this use of elliptic curves is not usually referred to as "elliptic curve cryptography."
>
> [...] As for other popular public key cryptosystems, no mathematical proof of difficulty has been published for ECC as of 2006. However, the U.S. National Security Agency has endorsed ECC technology by including it in its Suite B set of recommended algorithms. Although the RSA patent has expired, there are patents in force covering some aspects of ECC.

Note: Neal Koblitz is a math professor here at UW. He wrote the book on the congruent number problem (I scanned some of it for the website). You might see him around this summer, since he's teaching a summer school class.

Basic Problem: *How can people or computers send secret messages to each other without having to send out passwords ahead of time? How did mathematicians put the guys with briefcases handcuffed to their hands out of business?*

Sandor Kovacs will go into great detail about this question in his course, and you might view today as a preview of some of what he'll do, with the bonus that today you get to try it out on a computer. Today I'll just give you the chance to *understand and play with* one example that addresses this basic problem.

9.1 Elliptic Curves Modulo p

Let p be a prime number. Consider an equation $y^2 = x^3 + ax + b$ with

$$a, b \in \mathbb{F}_p = \{0, 1, \ldots, p-1\} \qquad \text{(integers modulo } p\text{)}$$

such that the cubic $x^3 + ax + b$ has distinct roots. The group of points on E modulo p is

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

Exercise: Make up several "random" elliptic curves over various random $\mathbb{F}_p$'s in SAGE (so *not* related to the congruent number problem!). List their points. Plot them. Do a little arithmetic with them. Here is some code to get you started.

Finding a random prime < 1000:

```
sage: next_prime(randrange(1000))
137
```

Making up a random curve:

```
sage: p = 137
sage: F = FiniteField(p)
sage: E = EllipticCurve(F, [F.random_element(), F.random_element()])
sage: print E
Elliptic Curve defined by y^2  = x^3 + 45*x + 43 over Finite Field of size 137
```

List all points:

```
sage: E.points()
[(0 : 1 : 0), (51 : 90 : 1), (57 : 92 : 1), (90 : 34 : 1), ...
```

Make a plot:

```
sage: show(plot(E, hue=.9))
```

Do some arithmetic:

```
sage: P = E.points()[1]  # first point listed above
sage: P
(51 : 90 : 1)
sage: P + P
(57 : 92 : 1)
sage: 10*P
(131 : 105 : 1)
sage: 9393*P
(129 : 26 : 1)
```

9.2 Computing nQ

Recall from yesterday that computers can compute $a^m \pmod n$ very quickly, even if m is **huge**. They do this by writing n in binary and doing a few squares and multiplies. Likewise, we can compute nQ quickly when Q is a point on an elliptic curve modulo p. Try it out!

```
sage: p = 137
sage: F = FiniteField(p)
sage: E = EllipticCurve(F, [F.random_element(), F.random_element()])
sage: P = E.random_element()
sage: print P
(96 : 94 : 1)

sage: time 102000823098320*P
(86 : 60 : 1)
CPU time: 0.12 s,  Wall time: 0.13 s

sage: show(plot(P) + plot(102000823098320*P,rgbcolor=(1,0,0)))
[[a plot]]
```

Now try with an elliptic curve over a huge field.

```
sage: p = next_prime(randrange(10^40))
sage: print p
sage: F = FiniteField(p)
sage: E = EllipticCurve(F, [F.random_element(), F.random_element()])
sage: P = E.random_element()
sage: print P
5541466958757039311365508431861627631 21
(49325762521836121109648490138966685669 0 :
         28686324803456248412855206922898457731 1 :
1)
```

Then multiply...

```
sage: time 909238403284092384209482038402*P
(151371634043111300277840422027192273952 :
       33373221337177148741228150653076417437 5 :
1)
CPU time: 0.20 s,  Wall time: 0.21 s
```

9.3 Diffie-Hellman – a way to create a shared secret

The Diffie-Hellman key exchange was the first ever public-key cryptosystem. We will try it out on a elliptic curve here (note: it can also be used directly in $\mathbb{F}_p^* = \{1, \ldots, p-1\}$, as you will learn in Sandor's course).

Public key cryptography involves three "people":

- Person 1 – traditionally named Alice
- Person 2 – traditionally named Bob
- Person 3 – traditionally called The Adversary

1. Break up into groups of (at least) 3. Choose at least person to be Alice[1], at least one to be Bob[2], and one to be the Adversary. Each person should have a computer terminal open to their SIMUW SAGE notebook. Open a common SAGE worksheet that all three of you can see and use to post messages (by refreshing the page). I'll explain how to do this.

2. In this exercise Alice and Bob will agree on a secret key by sending message *in full view* of everybody else. Of course, what they do at there computers gets kept secret – only the messages are public (in particular, Adversary should not look at the crypto worksheets of Alice and Bob).

3. Alice: Choose a random prime p and create a random elliptic curve modulo p, then choose a random point on this elliptic curve.

```
sage: load cong.sage # defines random_elliptic_curve command
sage: E = random_elliptic_curve(next_prime(randrange(1000)))
sage: print E
Elliptic Curve defined by y^2  = x^3 + 508*x + 42 over Finite Field of size 577

sage: P = E.random_element()
sage: P
(386 : 331 : 1)
```

   Finally, Alice has to tell everybody the random elliptic curve and the random point in such a way that Bob can define it on his computer. In the above example, just report that the prime is 47, that the curve is `EllipticCurve([36,3])`, and the point is $(5, 4)$.

4. Bob: Choose a random integer b (up to about p in size) and compute bP and tell everyone.

```
sage: b = randrange(1000); b
549

sage: b*P
(472 : 340 : 1)
```

   Announce $(83, 362)$ to the world. But keep b secret.

5. Alice: Do the same thing as Bob, but with your own integer a.

[1] Even a guy could be "Alice", e.g., there is a guy named Alice Cooper from Phoenix, AZ.
[2] Are there any famous women named Bob?

```
sage: a = randrange(1000); a
779

sage: a*P
(54 : 426 : 1)
```

6. Now for the key exchange. At this point everybody should know E, P, aP and bP. Only Alice knows a and only Bob knows b. Alice computes $a(bP)$ and Bob computes $b(aP)$. The Adversary, not knowing a or b, sits there frustrated. Meanwhile Alice and Bob have agreed on a shared secret.

```
sage: b*(a*P)
(260 : 99 : 1)

sage: a*(b*P)
(260 : 99 : 1)
```

7. Nonetheless, since the numbers are so small, the adversary *can* figure out a. E.g.,

```
Q = P
aP = E([54, 426])
for n in range(1,1000):
    if Q == aP:
        print n
        break
    else:
       Q = Q + P
```

   NOTE: There are better methods than the above simplistic brute force approach. But even the better methods aren't very good.

8. Go through each of the above steps, but with a much larger prime p, e.g., with 40 digits (basically just change all the 1000's above to 10^{40}'s). Note that it isn't noticeably slower. The only difference is that the Adversary's job is **much harder**.

Once you have a shared secret, you can use it to encrypt a message in various ways, many very complicated. A very simple way is to simply add (modulo 10 each digit of the shared secret key to the digits of your "message" (which we encode as a number).

9.4 A serious cryptosystem that was deployed: MS-DRM

There is another famous elliptic curve cryptosystem that involves elliptic curves. Read about it in detail in Section 6.4.2 of my book, which is at `http://modular.math.washington.edu/ent`.