Playing with Diophantine Equations, Math Circle, 4/30/06, O.Knill

1 Diophantine Equations

Equations with integer coefficients and integer solutions are called **Diophantine equations**. Examples are:

- $x^2 + y^2 = z^2$
- $x^4 + y^4 = z^4$
- $x^3 + y^3 = z^4$
- $x^2 + y^2 = 7z^2$
- $x^3 + 1 = y^2$

Mordell writes in the forword of his book: "For many centuries, no other topic has engaged the attention of so many mathematicians, both professional and amateur, or has resulted in so many published papers".

Research in Mathematics is mainly about solving open problems. Here are some open problems for Diophantine equations. Are there nontrivial solutions to the following Diophantine equations?

- $x^6 + y^6 + z^6 + u^6 + v^6 = w^6$
- $x^5 + y^5 + z^5 = w^5$
- $x^k + y^k = n!z^k, k \geq 2, n > 1$
- $x^a + y^b = z^c, a, b, c > 2, \gcd(a, b, c) = 1.$

Moral of this section: unsolved problems look simple and are a driving force for developing mathematics.

Problems for you:
1.1. can you find solutions to the linear Diophantine equation $7x + 4y = 10z$?
1.2. Why would a single nonzero solution to $x^6 + y^6 + z^6 + u^6 + v^6 = w^6$ lead automatically to infinitely many solutions?

Space to work:

2 A Construction from 1600 BC

One of the oldest results in Mathematics is the construction of **Pythagorean triples** $x^2+y^2 = z^2$. Lets do this:

Either x or y has to be even. Move the even one, say x^2 to the left and write $x^2 = z^2 - y^2 = (z - y)(z + y)$, then the right hand side contains a factor 4 and is of the form $4s^2t^2$. Therefore $2s^2 = z - y, 2t^2 = z + y$. Solving for z, y gives $z = s^2 + t^2, y = s^2 - t^2$, $x = 2st$.

For example, the choice of $s = 3, t = 2$ gives $x = 12, y = 5, z = 13$.

Moral of this section: Diophantine problems are old. Sometimes it is possible to parameterize the solution space.

Problems for you:
2.1. Why does either x or y have to be even if $x^2 + y^2 = z^2$?
2.2. Prove that there are infinitely many points (x, y) on the circle $x^2 + y^2 = 1$ for which x, y are rational points.

Space to work:

3 March into the Complex

Diophant already knew that if two numbers can each be written as a sum of two squares, then their product has this property also. In formulas, this is if $n = x^2 + y^2$ and $m = u^2 + v^2$, then $nm = a^2 + b^2$ for some integers. How do we find a and b?

With $z = x + iy$, $w = u + iv$. $zw = xu - yv + i(xv + yu)$. Because $|z|^2 = x^2 + y^2$, $|w|^2 = u^2 + v^2$, we have $|zw|^2 = |z^2||w^2| = (xu - yv)^2 + (xv + yu)^2$.

Moral of this section: Complex numbers are useful also in number theory.

Problems for you:
3.1. If n, m are both of the form $x^2 + 4y^2$, then their product nm can also be represented in this form.
3.2. If n, m are of the form $x^2 + y^2 + z^2 + w^2$, then nm is of that form too. You can prove this using quaternions $X = x + iy + jz + kw$, which satisfy $i^2 = j^2 = k^2 = -1$. You can use that quaternions have the property that the length $|X| = \sqrt{x^2 + y^2 + z^2 + w^2}$ has the property $|XY| = |X| \cdot |Y|$.

Space to work:

4 Local Properties

The equation $x^2 = 3 + 7y^2$ has no solution. How does one see that?

The key is to look at an equation modulo some number. If there is no solution on that reduction, then there is no solution at all. For the example, modulo 8, the equation is $x^2 + y^2 = 3$. But modulo 8, all squares are congruent to $0, 1, 4$. So the left hand side is congruent to $0, 1, 2, 5$. The right hand side is congruent to 3.

An equation which has solutions if it has solutions modulo p^n for all primes p satisfies the **Hasse principle**, which is also called the **global-local** principle.

Moral of this section: Look at the equation modulo p. This local property allows to show the nonexistence of solutions.

Problems for you:
4.1. Show that $x^2 + y^2 + z^2 = 7w^2$ has no solutions.
4.2. Show that $2x^2 + 3y^2 = z^2$ has no solutions (Davenport)
Here is a challenge: show that $y^2 = x^3 + 7$ has no solutions (Lebesque 1869)

Space to work:

5 Homer Simpson meets Fermat

Fermats theorem about the nonexistence of nontrivial solutions of $x^n + y^n = z^n$ with $n \geq 3$ has been proven about 10 years ago with surprisingly elaborate methods. The proof uses mathematical artillery which Fermat definitely had not available. The quest for a simple proof goes on and the internet is full of wrong proofs. In April 4 1994, an email by Henri Darmon has announced a counter example to the Fermat conjecture. It turned out to be a hoax. But here is counter example in Simpson TV series which you can try out: If you compute on a calculator or Mathematica $(1782^{12} + 1841^{12})^{(1/12)}$ you obtain 1922. What is wrong with that?

Moral of this section: Be careful when looking at proofs as well as counter examples.

Problems for you:
5.1. What is really going on with the above example?
5.2. Assume $x^p + y^p = z^p$ is not solvable. Why are there no solutions to $x^{kp} + y^{kp} = z^{kp}$ also?

Space to work:

6 The Super Fermat equation

The Texan banker Andrew Beals has sponsored a prize of $100'000$ dollars for a proof or counter example to the following statement:

"If $x^p + y^q = z^r$ with $p, q, r > 2$, then $\gcd(x, y, z) > 1$."

The problem is open. There was some controversy about who came up first with the problem. Beals has asked the problem at about the same time as some mathematicians have.

Moral of this section: Be careful when looking at proofs as well as counter examples. Also good conjectures can be worth a bounty.

Problems for you:
6.1. Why do we need the condition $q, p, r > 2$? Can you find examples? Say for $(q, p, r) = (2, 2, 3)$?

6.2. Why do we need $\gcd(q, p, r) = 1$ in the conjecture? Can you find examples?

Space to work: Here are some squares, cubes and bicubics

2	3	4
1	1	1
4	8	16
9	27	81
16	64	256
25	125	625

7 Cracking Secure Codes

Diophantine equations play a role, when trying to factor large integers n, a problem which has cryptological applications. While factorization can be restated as finding nontrivial solutions to $n = xy$, one can restate it also in other ways: if (x, y) solves the Diophantine equation $nx+y^2 = 1$, and $x, y < n$, then $y^2 - 1 = (y - 1)(y + 1)$ is a multiple of n so that $\gcd(y - 1, n)$ is a factor of n. The solution y is a square root of 1 modulo n. More generally, if one can find x such that x^2 is a small square y^2 modulo n, then the GCD of $x - y$ with n is a factor of n. Finding x for which x^2 is small modulo n is one of the **holy grails** to crack this encryption system. For example, to factor 51, we have to find x such that $x^2 = 1$ modulo 51. Indeed, $16^2 = 256 = 1 \bmod 51$ and $\gcd(15, 51) = 3$ is a factor. Or $35^2 = 1 \bmod 51$ we have $\gcd(34, 51) = 17$.

Any solutions to the Diophantine equation $y^2 = 2n^2 + xn + 1$ leads to a solution of $x^2 = 1 \bmod n$. Write $y = f(x) = \sqrt{2n^2 + xn + 1}$, then $\alpha = f'(x) \sim 1/\sqrt{2}$ and $f(x + 1) - f(x) \sim \alpha$.

Moral of this section: The topic of Diophantine equations can have implications for your daily life.

Problem for you:
7.1. Find x such that x^2 is 1 modulo $17 * 19$.
7.2. Factor $RSA - 704 = 74037563479561712828046796097429573142593188889231289084936232638972765034028266276891996419625117843995894330502127585370118968098286733173273108930900552505116877063299072396380786710086096962537934650563796359$ and win 30'000 dollars.

Space to work:

8 A Taxi Cab Number

Look at the Diophantine equation $x^3 + y^3 - z^3 = w^3$. Because $1/3 + 1/3 + 1/3 + 1/3 > 1$, we expect many solutions to this equation. Diophant himself already knew the solution $3^3+4^3-6^3 = 5^3$. Famous is the solution $1^3 + 12^3 - 6^3 = 10^3$ found by Bessy in 1657. It allows to write $1729 = 1^3 + 12^3 = 9^3 + 10^3$ in two different ways. This is the smallest number with this property. When Hardy visited Ramanujan in the hospital, he mentioned that the taxi had a boring number 1729. Ramanujan immediately pointed out that this is an important number, because of the above property. One calls Taxicab(k) the smallest number which is expressible in k different ways as sums of two cubes. Clearly Taxicab(1)=2. It is known that Taxicab(2)=1729. One knows Taxicab(3)=87539319 until Taxicab(5) and thinks that Taxicab(6)=24154419581254312065344.

Moral of this section: Even relatively small numbers can keep secrets.

Problems for you:
8.1. Verify that one can get solutions to $x^3 + y^3 + z^3 + w^3 = 0$ with the formulas $x = -(A - 3B)(A^2 + 3B^2) + 1$ $y = (A + 3B)(A^2 + 3B^2) - 1$ $z = (A^2 + 3B^2)^2 - (A + 3B)$ $w = -(A^2 + 3B^2)^2 + (A - 3B); x^3 + y^3 + z^3 + w^3$

8.2. Find a concrete solution to the Diophantine equation $x^2+y^2 = z^2+w^2$ for which x, y, z, w are all different.

Space to work:

9 The Elkies Equation

The equation $x^4 + y^4 + z^4 = w^4$ is a Diophantine equation from which Euler had thought that it has no solutions. But 1988, Noam Elkies at Harvard found the solution

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4 .$$

Euler already has found a solutions to $x^4 + y^4 = z^4 + w^4$: it is $x = 12231, y = 2903, z = 10381, w = 10203$.

Moral of this section: Also great minds can state wrong conjectures.

Problems for you:
9.1. Verify Elkies and Euler solutions are indeed solutions.
9.2. What would you consider to be a trivial solution to $x^4 + y^4 = z^4 + w^4$?

Space to work:

10 More Examples

The Diophantine equation $x^4 + y^4 - z^4 = 2w^2$ has solutions $x = u^2 - v^2, y = u^2 + v^2, z = 2uv, w = u^4 - v^4$. The equation $x^6 + y^6 + z^6 = u^6 + v^6 + w^6$ has solutions $(25, 62, 138, 82, 92, 135)$ (Montgomery) and $x^5 + y^5 = u^5 + v^5 + w^5$ has solutions $(14132, 220, 14068, 6247, 5027)$ The equation $y^2 = 2x^4 - 1$ is known to have only the solutions $(1, 1)$ and $239, 13)$ (Ljunggren 1966).

Moral of this section: there are tons of Diophantine problems still to be explored.

Problems for you:
10.1. Do you see a pattern? If we look at an equation $x_1^m \pm ... \pm x_k^m = 0$. What should the relation between m and k be, in order to expect a solution?
10.2. According to the rule, you just have developed, you predict that the equation $x^3 + y^3 + z^3 = w^3$ which has been studied by Diophant already has solutions. Find a solution

Space to work:

11 The Bigger Picture

Is there a general algorithm which decides whether a given Diophantine equation has a solution or not? This is the 10'th question in Hilbert's list of problems of 1900. The answer is now known to be "no".

Moral of this section: There are limits in mathematics, but exploring these limits has no limits.

Problems for you:
11.1. Is there a general algorithm which decides, whether a linear Diophantine equation has a solution or not?
11.2. Show that every system of Diophantine equations can be written as a single Diophantine equation.

Space to work:

12 The Pell Equation

Solving Diophantine equations is a problem in the field of dynamical systems also. Lets look at the example $x^2 - 1 = ay^2$ which is called the Pell equation. The points (x, y) which satisfy this equation are located on the graph of the function

$$f(x) = \frac{1}{\sqrt{a}}\sqrt{1 - x^2} \; .$$

Differentiation of f gives $f'(x) = \alpha x/\sqrt{x^2 - 1}$ and $f''(x) = -\alpha/(x^2 - 1)^{3/2}$, where $\alpha = 1/\sqrt{a}$. Quantization: If $f(x)$ is $1/(2x)$ close to an integer, then it is an integer. To obtain points close to the origin, we start with some point x_0 and add $k\alpha$ to $\beta = f(x_0)$ until $\beta + k\alpha$ is small. This can be done using the continued fraction expansion of α.

Moral of this section: The field of Diophantine systems has connections with other mathematical subjects like Chaos theory.

Problem for you:

12.1. Find a solution to the Pell equation $x^2 - 1 = 2y^2$.
12.2. Why are there no solutions to the Pell equation $x^2 + 2 = 9y^2$?

Space to work:

13 Symmetric Diophantine Equations

For $k > m$, the Diophantine equation $x_1^m + ... + x_k^m = y_1^m + ... + y_k^m$ has infinitely many solutions, for which $y_1, ..., y_k$ is not just a permutation of $x_1, ..., x_k$.
Proof. Define $f(x) = \sqrt{(x_1^m + ... + x_k^m)}$. Look at all the values f takes for integer points in $0 \leq x_i \leq n, 0 \leq y_i \leq n$. The image of f gives $n^k/k!$ numbers in $[0, (kn)^{m/2}]$. By the pigeon hole principle, there are two **different** x, y for which $f(x), f(y)$ has distance $\epsilon \leq k^{m/2} n^{m/2}/n^k$. Squaring $f(x) + \epsilon = f(y)$ gives $(f(x)^2 + \epsilon f(x) + \epsilon^2) = f(y)^k$. We have $|f(x)| \leq k^{m/2} n^{m/2}$ and $\epsilon \leq k^{m/2} n^{m/2}/n^k$. We know that $\epsilon f(x) + \epsilon^2$ is an integer Estimating its absolute value shows $\leq k^m n^{m-k} + k^m n^m / n^{2k}$ which must be 0 if n is larger than $2k^m$.

The simple proof shows that for every l and every $k > m$, there are examples, where one can write a number in l different ways as a sum of k different m.

Moral of this section: Even so number theory deals with discrete objects, some calculus and probabilistic thinking can help to get insight.

Problems for you:

13.1. Prove the following corollary: the Euler Diophantine equation $x_1^m + ... + x_k^m = x_0^m$ has nontrivial solutions if k is odd and $k + 1 \geq 2m$.

13.2. Repeat the proof in detail in the case $m = 2$ and $k = 3$ to show that there is a solution $0 < x < y < z < 18$, $0 < a < b < c < 18$ with $(x, y, z) \neq (a, b, c)$ to $x^2 + y^2 + z^2 = a^2 + b^2 + c^2$.

Space to work:

14 Eulers Diophantine Equation

The Diophantine equation $x_1^m + ... + x_k^m = x_0^m$ is called **Eulers Diophantine equation**. Here is a heuristic argument: for $x_i \leq n^{1/m}$, there are $n^{1/m} n^{1/m} \cdots n^{1/m} = n^{k/m}$ numbers. Each of them gives rise to a real number $(x_1^m + ... + x_k^m)^{1/m} \bmod 1$ in $[0, 1)$. We expect one to be $1/n^{k/m} = n^{m/k}$ close to 0.

How close do we have to be? If $x + \epsilon = 0$, then $(x + \epsilon)^m$ is an integer. Because this is $x^{m-1}\epsilon$ plus an integer and smaller terms, we know that if $x^{m-1}\epsilon < 1$, then $\epsilon = 0$. So, the threshold is $x^{m-1} = n^{(m-1)/m}$.

Moral of this section: probabilistic thinking can help to bring order into the zoo of Diophantine equations.

Problems for you:

14.1. Is it true that the Euler Diophantine equation has solutions for $k >= m - 1$ and no solutions for $k < m - 1$?
14.2. What happens for $k = m - 1$? $k = 2, m = 3$ is not impossible (Fermat), $k = 3, m = 4$ is possible (Elkies), $k = 4, m = 5$ has solutions (Lander Parkin) , $k = 5, m = 6$ is open.

Space to work:

15 Solutions to the Problems

1.1 $(x, y, z) = (4, 3, 4)$ works.
1.2. (kx, ky, kz, ku, kv) are also solutions.

2.1. Look at the equation $x^2 + y^2 = z^2$ modulo 4. If x, y would both be odd, then $x^2 = 1, y^2 = 1$ modulo 4 and the sum would be 2 modulo 4. But 2 is not a square modulo 4.
2.2. Divide the equation $x^2 + y^2 = z^2$ by z^2 to obtain $(x/z)^2 + (y/z)^2 = 1$.

3.1 Complex numbers $z = x + 2yi$ have the property that $|z|^2$ is of the form $x^2 + 4y^2$. If we multiply two such complex numbers, $z = x + 2yi$, $w = u + 2vi$, we obtain $zw = xu - 4yv + i(2xv + 2yu) = a + 2ib$.
3.2 The fact that the norm of two quaternions is the product of the norms can best be seen in linear algebra.

4.1. Look at this equation modulo 8. Modulo 8, each square $0, 1, 4, 9, 16, 25, 36, 49, 64$ is either congruent to 0 or 1 or 4. If we add three squares, we only can reach $0, 1, 2, 3, 4, 5, 6$ but not 7.
4.2 We can assume that x, y, z have no common denominator. Look at the equation modulo 3, where each square is either 0 or 1. So, the left hand side is either 0 or 2, the right hand side is either 0 or 1. But if x, z are both divisible by 3, then also y must be divisible by 3 and we would have a common denominator.
The challenge: First of all, x must be odd, otherwise look modulo 8. The equation $y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4) = (x + 2)((x - 1)^2 + 3)$ second factor is of form 4k+3 So is each prime factor q of the second factor. Look at the equation modulo 4.

5.1. The result is correct only for a few digits. With 20 digits, it gives 1921.9999999558672254.
5.2 Assume you have proven Fermat for prime p and n is an integer which contains the prime factor p, then $n = pq$. We can not solve $x^n + y^n = z^n$ because with $X = x^q, Y = y^q, Z = z^q$, we had $X^p + Y^p = Z^p$ which we know to be false.

6.1 Examples are $1^2 + 2^3 = 3^2$, $2^5 + 7^2 = 3^4$ and $7^3 + 13^2 = 2^9$.
6.2. Examples are $2^3 + 2^3 = 2^4$ or $3^9 + 54^3 = 3^{11}$.

7.1. $18^2 - 1 = (18 - 1)(18 + 1)$ is zero modulo 17*19.
7.2. I wish, I would know that. Could need the cash!

8.1. This is a direct computation. Here it is done in Mathematica

```
x = -(A-3B) (A^2 + 3 B^2) + 1;
y = (A+3B) (A^2 + 3 B^2) - 1;
z = (A^2+ 3B^2)^2 - (A+3B);
w= -(A^2 + 3B^2)^2 + (A-3B); Simplify[x^3+y^3+z^3+w^3]
```

8.2. here is a solution: $6^2 + 17^2 = 10^2 + 15^2$.

9.1. best done with a computer.
9.2. If $(x, y) = (z, w)$ or $(x, y) = (w, z)$.

10.1 We expect solutions if $k > m$ and no solutions if $k < m$. Here are some examples:

Equation name	below rule of thumb	border line	rule of thumb holds	∃
Babylon			$x^2 + y^2 = z^2$	x
Fermat	$x^4 + y^4 = z^4$			-
Fermat		$x^4 + y^4 = z^2$		-
Catalan	$x^2 + 1 = z^3$			-
Elkies		$x^4 + y^4 + z^4 = w^4$		x
Pell		$x^2 - dy^2 = 1$		x
Prestet			$x^3 + y^3 + z^3 = w^3$	x
234 equation			$x^2 + y^3 = z^4$	x
Lander Parkin		$x^5 + y^5 + z^5 + v^5 = w^5$		x
Euler	$x^5 + y^5 + z^5 = w^5$			?
Euler		$x^6 + y^6 + z^6 + u^5 + v^6 = w^5$		?

Tues theorem says that for $k = 2$, a homogeneous equation $f(x, y) = n$ of degree $m > 2$ has only finitely many solutions.

10.2. One of the smallest solutions is $3^3 + 4^3 + 5^3 = 6^3$.

11.1. Yes for linear Diophantine equations, we can decide. Let $5x = 3y = 7z$. This means $5x + 3y = 0$ modulo 7. There is a solution if and only if one of the coefficients a satisfies $\gcd(a, 7) = 1$.
11.2. Lets take the case of two equations $f = 0, g = 0$. This system is equivalent to the single equation $f^2 + g^2 = 0$.

12.1. $x^2 - 1 = 2y^2$ has the solution $(3, 2)$.
12.2 Rewrite it as $x^2 + 2 = 9y^2 = z^2$, with $z = 3y$. But the equation $x^2 + 2 = z^2$ has no solutions, because the list of possible differences between two squares is $0, 1, 3, 4, ...$

13.1 If k is odd, we can take some powers on the other side.
13.2. Define $f(x, y, z) = \sqrt{x^2 + y^2 + z^2}$ on the set $(x, y, z), 0 < x < y < z \leq n$. It contains $n^3/6$ integer lattice points. The function takes values in $[1, \sqrt{3}n]$. There are two vectors (x, y, z) and (a, b, c) for which $f(x, y, z) = f(a, b, c) + \epsilon$ with $\epsilon \leq 6\sqrt{3}/n^2$. Squaring gives

$$f(x, y, z)^2 = f(a, b, c)^2 + 2\epsilon f(a, b, c) + \epsilon^2$$

and shows that $2\epsilon f(a, b, c) + \epsilon^2$ is an integer. But it can be estimated by

$$\leq (\sqrt{3}n)(6\sqrt{3}/n^2) + (6\sqrt{3}/n^2)^2 \leq 18/n + 108/n^4$$

which is smaller than 1 for $n = 19$.

14.1 This is a research problem.

14.2 Also this is a research problem. Try $x^6 + y^6 + z^6 + u^6 + v^6 = w^6$.

---

16 To the Literature

There are tons of books about Diophantine equations. To prepare for this math circle lecture, I used [1, 3, 2, 5, 4]. They all are accessible on the high school level. Much of the modern research is more algebraic. This manifests itself that not integer solutions bur rational solutions are the focus of interest. While we have seen here, that looking for rational and integer solutions can be the same task (like for homogeneous equations), this is a totally different story in general. There are many equations which have only finitely many integer solutions but infinitely many rational solutions. Diophant himself looked also for rational solutions. But today, it is sometimes said that looking for rational solutions is rooted more in algebra, while looking for integer solutions is rooted more in number theory. There is of course a heavy overlap. The algebraic texts are in general much more abstract and not so easily accessible for high school students.

References

[1] Isabella Bashmakova. *Diophantus and Diophantine Equations*, volume 20 of *Dolciani Mathematical Expositions*. The Mathematical Association of America, 1997.

[2] L.E. Dickson. *History of the theory of numbers. Vol. II: Diophantine analysis*. Chelsea Publishing Co., New York, 1966.

[3] Richard K. Guy. *Unsolved Problems in Number Theory*. Springer, Berlin, 3 edition, 2004.

[4] L.K. Hua. *Introduction to Number theory*. Springer Verlag, Berlin, 1982.

[5] L.J. Mordell. *Diophantine Equations*, volume 30 of *Pure and Applied Mathematics*. Academic Press, London and New York, 1969.