Pythagorean Triples
○○○○○○○○○

Divisibility
○○○○○○○○○

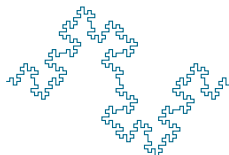Solving Linear Equations in Integers
○○○○○○

Cryptographic Mathematics I
Pythagorean Triplets

Dr. Eberhard Mayerhofer

University of Limerick

Semester I 2023/24

STRUCTURE

- ▶ Mathematical Course. Mostly "Elementary Number Theory", including Elliptic curves.
- ▶ Literature: "A friendly introduction to Number Theory" by Joseph H Silverman.
- ▶ Tutorial Videos on Tutorial Questions. Lab questions answered by students (Live).
- ▶ Assessment:
  - ▶ Project Week 8 - Group Work, contributing 20%
  - ▶ Final Test Week 12, 20%
  - ▶ Final Exam 60%.
- ▶ Syllabus: MA6011, www.bookofmodules.ul.ie.

Pythagorean Triples
○○○○○○○○○

Divisibility
○○○○○○○○○○

Solving Linear Equations in Integers
○○○○○○

Pythagorean Triples
OOOOOOOOO

Divisibility
OOOOOOOOO

Solving Linear Equations in Integers
OOOOOO

NUMBER SETS

▶ Natural numbers $\mathbb{N} := \{0, 1, 2, 3, \ldots, \}$.

▶ Integers $\mathbb{Z} := \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots, \}$.

▶ Rational numbers $\mathbb{Q}$: fractions of the form m/n, where m, n are integers, $n \neq 0$.

▶ Algebraic numbers: Solutions ("Roots") of algebraic equations. For example, x solving

$$ax^2 + bx + c = 0, \quad a, b, c \in \mathbb{Q}.$$

▶ Question: Is a rational number algebraic? Explain your answer!

▶ Up to fourth order, there are explicit formulas for algebraic numbers in terms of n-th roots.

► Irrational numbers: Not rational, e.g., $\sqrt{2}$ or π.

► Transcendental numbers: Not algebraic, e.g., π.

► Real numbers $\mathbb{R}$: any point on the real line, the collection of rational and irrational numbers.

► Complex Numbers: To make any algebraic equation solvable (at least one root), one introduces the imaginary unit $i := \sqrt{-1}$, and defines a complex number $z = a + bi$, where $a, b \in \mathbb{R}$.

EXAMPLE: DEPICT INTEGERS $-3, -2, -1, 0, 1, 2, 3$ ON REAL LINE

EXAMPLE: DEPICT THE RATIONAL NUMBER 2/3 ON THE REAL LINE. (HINT: USE THE INTERCEPT THEOREM!

EXAMPLE: DEPICT THE ALGEBRAIC (WHY?) NUMBERS $\pm\sqrt{2}$.

DEFINITION

The Babylonians discovered **Pythagorean triples** i.e. numbers
a, b, c satisfying

$$a^2 + b^2 = c^2.$$

► Geometric Interpretation ?
► Most popular: $(3, 4, 5)$
► Others: $(5, 12, 13), (7, 24, 25), (8, 15, 17)$
► There are infinitely many solutions.

Introducing the rational numbers $x = a/c$ and $y = b/c$, we can write the equation as

$$x^2 + y^2 = 1.$$

- Find all Pythagorean triples $\Leftrightarrow$ find all points on the unit circle (why?) which have rational coordinates (x, y).
- Since we have squares, it is sufficient to find all positive solutions (please mark the relevant part of the unit circle)
- There are four obvious points on the circle $x^2 + y^2 = 1$ (Which?).

Pythagorean Triples
○○●○○○○○○

Divisibility
○○○○○○○○○○

Solving Linear Equations in Integers
○○○○○○

ILLUSTRATION

Pythagorean Triples
○○○●○○○○○

Divisibility
○○○○○○○○○

Solving Linear Equations in Integers
○○○○○○

GEOMETRIC APPROACH

Let $P = (-1, 0)$ and let $m = p/q$, where $p \geq 0$ and q are integers and $q > 0$).

Consider the line through P with slope m. The equation of this line is

$$y - 0 = m(x + 1). \qquad (Why?)$$

This line will intersect the circle at a second point Q.

Pythagorean Triples
○○○○●○○○○

Divisibility
○○○○○○○○○○

Solving Linear Equations in Integers
○○○○○○

ILLUSTRATION

Pythagorean Triples
○○○○○●○○○

Divisibility
○○○○○○○○○

Solving Linear Equations in Integers
○○○○○○

FINDING Q

ALL RATIONAL SOLUTIONS OF $x^2 + y^2 = 1$.

▶ Any point constructed in this way is of the form

$$Q = \left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2} \right). \tag{1}$$

▶ Since m is rational, the coordinates of Q are also rational.

▶ Conversely, if we start with a point Q on the circle with rational coordinates then the slope of the line PQ is rational, hence we have determined all the points on the circle $x^2 + y^2 = 1$ with rational coordinates.

Pythagorean Triples
○○○○○○○●○

Divisibility
○○○○○○○○○

Solving Linear Equations in Integers
○○○○○○

HOW TO GET ALL (INTEGER) SOLUTIONS OF $a^2 + b^2 = c^2$?

▶ Any rational number m can be written as $m = v/u$ with u, v integers. Plugging this into (1) yields:

▶ Leads us to the equation

$$(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2$$

from which we see that

$$a = u^2 - v^2 \qquad b = 2uv \qquad c = u^2 + v^2$$

is a Pythagorean triple.

▶ By substituting for u and v we can find Pythagorean triples, as shown in the table below.

Pythagorean Triples
○○○○○○○○●

Divisibility
○○○○○○○○○

Solving Linear Equations in Integers
○○○○○○

u	2	3	4	4	5	5	6	6	7	7	7
v	1	2	1	3	2	4	1	5	2	4	6
a	3	5	15	7	21	9	35	11	45	33	13
b	4	12	8	24	20	40	12	60	28	56	84
c	5	13	17	25	29	41	37	61	53	65	85

- ▶ The triples (a, b, c) in this table are such that a, b, c don't have a common factor.

- ▶ Of course, if (a, b, c) is a Pythagorean triple and k a positive integer, then (ka, kb, kc) is another Pythagorean triple.

- ▶ Fermat's Last Theorem:

$$a^n + b^n = c^n$$

has no solutions in positive integers if $n \geq 3$. Fermat conjectured this in the 17th century.

DEFINITION

Let *m* and *n* be integers with $m \neq 0$. We say *m* divides *n* if *n* is a multiple of *m* i.e. there exists an integer *k* such that $n = km$.
If *m* divides *n* we write $m \mid n$.

Example

Thus

$$2 \mid 60 \text{ and } 3 \mid 60 \text{ and } 5 \mid 60 \text{ and } 10 \mid 60$$

A number that divides *n* is called a **divisor** of *n*.

BASIC OBSERVATIONS

- ▶ All positive divisors of n are less than or equal to $|n|$.
- ▶ Hence only finite number of divisors.
- ▶ Always 1 is a divisor of every integer n.

Thus if we take two integers m and n, the set of integers which are divisors of both m and n is a non-empty finite set and has a largest element which is called the **greatest common divisor** of m and n abbreviated to $\gcd(m, n)$. If $\gcd(m, n) = 1$ we say m and n are **coprime**.

Pythagorean Triples
○○○○○○○○○

Divisibility
○○●○○○○○○

Solving Linear Equations in Integers
○○○○○○

HOW DO WE CALCULATE $\gcd(m, n)$?

- ▶ (basic, not efficient) list all the divisors of m and n and take the largest number which is in both lists.
- ▶ (not efficient, either): List all prime divisors, and find the common ones (including powers of the same prime)
- ▶ (**Euclidean algorithm**, efficient). It involves doing a sequence of divisions with remainder until the remainder is zero.

DIVISION WITH REMAINDER

- Let m and q be integers.
- We can always write $m = q \times n + r$.
    - m is the dividend
    - n is the divisor
    - q is the (integer!) quotient
    - r is the integer remainder
- Practice: we take the integer part of m/n as q and then calculate $r = m - n \times q$.

EUCLIDEAN ALGORITHM (EXAMPLE 1)

Let $m = 126$ and $n = 1812$. Divide 126 into 1812.

$$1812 = 14 \times 126 + 48$$
$$126 = 2 \times 48 + 30$$
$$48 = 1 \times 30 + 18$$
$$30 = 1 \times 18 + 12$$
$$18 = 1 \times 12 + 6$$
$$12 = 2 \times 6$$

The Euclidean algorithm tells you that when you find a remainder of 0 then the greatest common divisor is the remainder in the previous step. Hence

$$\gcd(1812, 126) = 6.$$

Pythagorean Triples
○○○○○○○○○

Divisibility
○○○○○●○○○

Solving Linear Equations in Integers
○○○○○○

WHY DOES THE EUCLIDEAN ALGORITHM WORK?

Assume $a > b > 0$ and let the sequence of steps be as follows:

$$a = q_1 \times b + r_1$$
$$b = q_2 \times r_1 + r_2$$
$$r_1 = q_3 \times r_2 + r_3$$
$$\vdots$$
$$r_{n-2} = q_n \times r_{n-1} + r_n$$
$$r_{n-1} = q_{n+1} \times r_n + 0$$

For some n, $r_{n+1} = 0$ (Why?). Now $r_n \mid r_{n-1}$ and working upwards we find $r_n \mid r_{n-2}$... Eventually, we find that $r_n \mid r_1$ and $r_n \mid b$.

Finally from the first equation we find that $r_n \mid a$ and $r_n \mid b$ i.e. r_n is a common divisor of a and b.

And working down we see that any common divisor of a and b is a divisor of successively $r_1, r_2, r_3, \ldots, r_n$. Thus r_n is the greatest common divisor of a and b.

EFFICIENCY

- ▶ Number of steps in the Euclidean algorithm $\leq$ seven times the number of digits in b.

- ▶ Thus Euclidean algorithm calculations are easily done on a computer with numbers having thousands of digits.

- ▶ Improved version of the Euclidean algorithm called the **binary GCD algorithm**. It is based on the fact that if m and n are both even then $\gcd(m, n) = 2\gcd(m/2, n/2)$ while if m is even and n odd, $\gcd(m, n) = \gcd(m/2, n)$. In binary, division by 2 is a simple shift operation.

Pythagorean Triples
○○○○○○○○○

Divisibility
○○○○○○○●○

Solving Linear Equations in Integers
○○○○○○

BINARY GCD ALGORITHM ($\rightarrow$ EXAMPLE 1)

$$\begin{aligned}
\gcd(87654321, 12345678) &= \gcd(87654321, 6172839) \\
&= \gcd(14 \times 6172839 + 1234575, 6172839) \\
&= \gcd(6172839, 1234575) \\
&= \gcd(4 \times 1234575 + 1234539, 1234575) \\
&= \gcd(1234575, 1234539) \\
&= \gcd(1235439 + 36, 1234539) \\
&= \gcd(1234539, 36) \\
&= \gcd(1234539, 18) \\
&= \gcd(1234539, 9) \\
&= \gcd(9 \times 137171, 9) = 9
\end{aligned}$$

PROPERTIES

1. If $m \mid a$ and $m \mid b$ then $m \mid a + b$ and $m \mid a - b$.
2. If $m \mid a$ then $m \mid ka$ where k is an integer. Combining with 1) we have if $m \mid a$ and $m \mid b$ then $m \mid ka \pm lb$ for any integers k and l.
3. If $a \mid b$ and $b \mid c$ then $a \mid c$.
4. If $a \mid b$ and $c \mid d$ then $ac \mid bd$.
5. If $m \neq 0$ then $a \mid b \iff ma \mid mb$.
6. If $d \mid a$ and $a \neq 0$ then $|d| \leq |a|$.
7. $a \mid b$ and $b \mid a$ if and only if $a = \pm b$

Let a and b be integers. One can ask the question: What integers can be written in the form $ax + by$ with x and y integers? Take $a = 24$ and $b = 66$. We can draw up a table of values of $24x + 66y$ for small values of x and y

$y \backslash x$	-4	-3	-2	-1	0	1	2	3	4
-4	-360	-336	-312	-288	-264	-240	-216	-192	-168
-3	-294	-270	-246	-222	-198	-174	-150	-126	-102
-2	-228	-204	-180	-156	-132	-108	-84	-60	-36
-1	-162	-138	-114	-90	-66	-42	-18	6	30
0	-96	-72	-48	-24	0	24	48	72	96
1	-30	-6	18	42	66	90	114	138	162
2	36	60	84	108	132	156	180	204	228
3	102	126	150	174	198	222	246	270	294
4	168	192	216	240	264	288	312	336	360

Pythagorean Triples
○○○○○○○○○

Divisibility
○○○○○○○○○

Solving Linear Equations in Integers
○●○○○○

OBSERVATIONS

▶ Every entry in the table is a multiple of 6 which is $\gcd(24, 66)$

▶ 6 also appears in the table as

$$6 = 3 \times 24 - 1 \times 66.$$

▶ Conclude: smallest positive value in our table is the $\gcd(a, b)$.

This is true in general. Such an expression can be obtained from the Euclidean algorithm calculations to find the GCD.

$$
\begin{array}{ll}
66 = 2 \times 24 + 18 & 66 - 2 \times 24 = 18 \\
24 = 1 \times 18 + 6 & 24 - 1 \times 18 = 6 \\
18 = 3 \times 6 & 18 - 3 \times 6 = 0
\end{array}
$$

Pythagorean Triples
○○○○○○○○○

Divisibility
○○○○○○○○○

Solving Linear Equations in Integers
○○●○○○

On the right we have rewritten the equations to have the remainders alone on the right hand side. Substituting in the second equation for 18 the left hand side of the first equation, we get

$$6 = 24 - 1 \times 18 = 24 - 1 \times (66 - 2 \times 24) = 3 \times 24 - 1 \times 66$$

One can also work forwards. From the first equation $18 = a - 2b$ where $a = 66$ and $b = 24$. The second equation becomes $b - (a - 2b) = 6$ from which we again obtain $6 = 3b - a = 3 \times 24 - 1 \times 66$.

Pythagorean Triples
OOOOOOOOO

Divisibility
OOOOOOOOO

Solving Linear Equations in Integers
OOO●OO

▶ Thus the linear equation $ax + by = \gcd(a, b)$ has a solution in integers x_0 and y_0, found by the EEA.

▶ We can create other solutions as follows.

$$ax_0 + by_0 = d \Rightarrow ax_0 + kab + by_0 - kab = a(x_0 + kb) + b(y_0 - ka) = d$$

Thus $(x_0 + kb, y_0 - ka)$ is another solution.

As result we obtain the following.

Theorem

Let a and b be non-zero integers with $\gcd(a, b) = d$. The equation

$$ax + by = d$$

has a solution (x_0, y_0) in integers which can be found by means of the extended Euclidean algorithm. Every solution of this equation can be obtained by substituting integers k into the formula

$$\left(x_0 + k\frac{b}{d}, y_0 - k\frac{a}{d} \right). \tag{2}$$

A simple extension is the following:

Theorem

Let a and b and c be non-zero integers, with $\gcd(a, b) = d$. *The equation*

$$ax + by = c$$

has a solution if and only if $d \mid c$.

Prove the statement and provide a formula for all solutions similar to the previous slide (there are either none, or countably many.)

Hint

If c is not divisible by d, there cannot be a solution (why?). Conversely, if c is divisible by d, we can construct a solution of $au + bv = d$ (How?) and then get $x_0 = uc/d$ and $y_0 = vc/d$. That all solutions are of the form (2) is proved in the same way as the previous theorem.