Diophantine Equations

Diophantus of Alexandria (Ancient Greek: Διόφαντος ὁ Ἀλεξανδρεύς; born probably sometime between AD 201 and 215; died around 84 years old, probably sometime between AD 285 and 299), sometimes called "the father of algebra", was an Alexandrian Greek mathematician[1][2][3][4] and the author of a series of books called *Arithmetica*, many of which are now lost. These texts deal with solving algebraic equations. While reading Claude Gaspard Bachet de Méziriac's edition of Diophantus' *Arithmetica,* Pierre de Fermat concluded that a certain equation considered by Diophantus had no solutions, and noted in the margin without elaboration that he had found "a truly marvelous proof of this proposition," now referred to as Fermat's Last Theorem. This led to tremendous advances in number theory, and the study of Diophantine equations ("Diophantine geometry") and of Diophantine approximations remain important areas of mathematical research. Diophantus coined the term παρισότης (parisotes) to refer to an approximate equality.[5] This term was rendered as *adaequalitas* in Latin, and became the technique of adequality developed by Pierre de Fermat to find maxima for functions and tangent lines to curves. Diophantus was the first Greek mathematician who recognized fractions as numbers; thus he allowed positive rational numbers for the coefficients and solutions. In modern use, Diophantine equations are usually algebraic equations with integer coefficients, for which integer solutions are sought.

Sophie Germain

This article is about the mathematician Marie-Sophie Germain. For the number theory (set, or predicate), see Sophie Germain prime.

Marie-Sophie Germain (French: [maʁi sɔfi ʒɛʁmɛ̃]; 1 April 1776 – 27 June 1831) was a French mathematician, physicist, and philosopher. Despite initial opposition from her parents and difficulties presented by society, she gained education from books in her father's library including ones by Leonhard Euler and from correspondence with famous mathematicians such as Lagrange, Legendre, and Gauss. One of the pioneers of elasticity theory, she won the grand prize from the Paris Academy of Sciences for her essay on the subject. Her work on Fermat's Last Theorem provided a foundation for mathematicians exploring the subject for hundreds of years after.[1] Because of prejudice against her sex, she was unable to make a career out of mathematics, but she worked independently throughout her life.[2] Before her death Gauss had recommended that she be awarded an honorary degree, but that never occurred.[3] At the centenary of her life, a street and a girls school were named after her. The Academy of Sciences established the Sophie Germain Prize in her honor.

Marie-Sophie Germain

$a, b \in \mathbb{N}$

$\gcd(a,b)$ = greatest common divisor of a & b is d s.t. $d \mid a$, $d \mid b$ and d is the largest of all numbers with those properties.

<u>How to find?</u>

Stupid Algorithm: Factor a, b; chose largest power of each prime common to both.

<u>Example</u>: $\gcd(60, 90)$

$$\left.\begin{array}{l} 60 = 2^2 \times 3 \times 5 \\ 90 = 2 \times 3^2 \times 5 \end{array}\right] \gcd = 2 \times 3 \times 5 = 30.$$

<u>Better Method</u> Euclid's Algorithm:

Let $a > b$. If not just switch them.

Write $a = q_1 b + r_1$

We know we can do this for $q_1, r_1 \in \mathbb{Z}$

More over we can always take $r_1 < b$. If not, just increase q_1.

$q_1 \geq 0$, $r_1 \geq 0$

Now write

$$b = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$
$$r_2 = q_4 r_3 + r_4$$
$$\vdots$$
$$r_{n-2} = q_n r_{n-1} + r_n$$
$$r_{n-1} = q_{n+1} r_n + 0.$$

<u>Claim</u> $r_n = \gcd(a,b)$.

<u>First</u> $r_n \mid a$ and $r_n \mid b$

<u>proof</u> Since $r_{n-1} = q_{n+1} r_n$, $r_n \mid r_{n-1}$. Now

$r_{n-2} = q_n r_{n-1} + r_n$ and $r_n \mid r_{n-1}$ and $r_n \mid r_n$ so $r_n \mid r_{n-2}$.

By induction, $r_n \mid r_{n-1}$, $r_n \mid r_{n-2}$, $\ldots$, $r_n \mid r_1$

$b = q_2 r_1 + r_2$, $r_n \mid r_1$, $r_n \mid r_2 \Rightarrow r_n \mid b$.

$a = q_1 b + r_1$, $r_n \mid b$, $r_n \mid r_1 \Rightarrow r_n \mid a$.

So r_n is a common divsor.

Let $d \mid a$ and $d \mid b$.

Then since

$a = q_1 b + r_1$, $r_1 = a - q_1 b$

so $d \mid r_1$.

$b = q_2 r_1 + r_2$, $r_2 = b - q_2 r_1$

and $d \mid b$ and $d \mid r_1 \Rightarrow d \mid r_2$

$r_1 = q_3 r_2 + r_3$, $r_3 = r_1 - q_3 r_2$

$d \mid r_1$, $d \mid r_2 \Rightarrow d \mid r_3$

$\vdots$

By induction

$d \mid a$, $d \mid b$, $d \mid r_1$, $\ldots$, $d \mid r_{n-1}$

$r_{n-2} = q_n r_{n-1} + r_n$, $r_n = r_{n-2} - q_n r_{n-1}$

So $d \mid r_n$. Hence any common divisor of a and b divides r_n, so r_n is the greatest common divisor.

By the way, we know the process terminates since $a > b > r_1 > r_2 > r_3 > \cdots > r_n > 0$

<u>Fact</u> $r_{k+2} < \frac{r_k}{2}$

<u>proof</u> $r_k = q_{k+2} r_{k+1} + r_{k+2}$

If $\quad r_{k+2} \geq \frac{r_k}{2}$, then

$$r_k = q_{k+2} r_{k+1} + r_{k+2} > q_{k+2} r_{k+2} + r_{k+2}$$

$$\geq q_{k+2} \frac{r_k}{2} + \frac{r_k}{2} \geq r_k$$

So $r_k > r_k$ a contradiction.

Hence $r_{k+2} < \frac{r_k}{2}$. So every second iteration the remainder decreases by a factor of 2. Hence the process will end after $2 \log_2 b$

The 2 is because its only every second iterate that decreases by a factor of 2. $\log_2$ because of this factor of 2. $2 \log_2 b = 2 \log_2 10 \log_{10} b$

Using the change of base formula for logarithms: $\log_a x = \dfrac{\log_b(x)}{\log_b(a)}$

$$7 < 2 \log_2 10 < 8.$$