Lecture 1

(Primes as) Sums of squares

Let p be a prime. In this chapter, we want to solve

$$x^2 + y^2 = p, \quad x, y \in \mathbb{N}$$

if possible.

Ex.

$$5 = 2^2 + 1^2$$
$$13 = 3^2 + 2^2$$
$$17 = 4^2 + 1^2$$
$$29 = 5^2 + 2^2$$

Non-Ex. We can not solve

$$x^2 + y^2 = 3$$
$$x^2 + y^2 = 7.$$

Q. Can you guess for which primes we can solve the above and for which prime we can't?

A. Indeed, there is a pattern.

Proposition

Let p be a prime with $p \equiv 3 \bmod 4$. Then $x^2+y^2 = p$ has no solutions in $(x, y) \in \mathbb{Z}^2$.

Proof: check the mod 4 table

$x \bmod 4$	$x^2 \bmod 4$	$y^2 \bmod 4$	$x^2+y^2 \bmod 4$
0	0	0	0
1	1	0	1
2	0	1	1
3	1	1	2

Thus $x^2+y^2 \not\equiv 3 \bmod 4$ for any pair of $(x, y) \in \mathbb{Z}^2$. ∎

Rmk: $p \equiv 2 \bmod 4$ & p is prime $\Rightarrow p = 2$. Then $1^2+1^2 = 2$. Thus we may concentrate on $p \equiv 1 \bmod 4$

Theorem: If $\left(\frac{-1}{p}\right) = 1$ then $x^2+y^2 = p$ has solutions in $(x, y) \in \mathbb{Z}^2$.

Corollary: If $p \equiv 1 \bmod 4$ then $x^2 + y^2 = p$ is solvable in $x, y \in \mathbb{Z}$.

Proof: Note that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

If $p \equiv 1 \bmod 4$ then $\frac{p-1}{2}$ is even.

So, $\left(\frac{-1}{p}\right) = 1$. Thus the theorem implies $x^2 + y^2 = p$ solvable. ☒

Proof of the theorem:

First we prove a lemma.

Lemma: Let $\alpha \in \mathbb{R}$ & $N \in \mathbb{N}$. Then $\exists\ \frac{s}{t} \in \mathbb{Q}$ with $GCD(s,t) = 1$ and $1 \le t \le N$ s.t. $\left|\alpha - \frac{s}{t}\right| < \frac{1}{t(N+1)}$

RMK: The above lemma is also known as Dirichlet's approximation theorem.

Proof of lemma

Let $r = [a; a_1, \dots]$ either finite or infinite and $r_n = \frac{s_n}{t_n}$ be its n'th convergent.

We saw in week 6 that

$$|r - r_n| = \left|r - \frac{s_n}{t_n}\right| \leq |r_{n+1} - r_n| \leq \frac{1}{t_n t_{n+1}}.$$

If $t_{n+1} \geq N+1$ for some $n \in \mathbb{N}$, then

$$\left|r - \frac{s_n}{t_n}\right| \leq \frac{1}{t_n (N+1)},$$

i.e. $\frac{s_n}{t_n}$ is the required rational.

If $t_{n+1} < N+1$ for all $n \in \mathbb{N}$ then t_n - sequence must stabilize as t_n is an increasing sequence.

This is only possible if the continued fraction expansion is finite $\Leftrightarrow r \in \mathbb{Q}$.

Thus $r = \frac{s}{t}$ with $GCD(s, t) = 1$

But then $\left|r - \frac{s}{t}\right| = 0 \leq \frac{1}{t(N+1)}$. ☐

Proof of the theorem

As $\left(\frac{-1}{p}\right) = 1$, i.e. -1 is a quadratic residue mod p. Hence, $\exists\, z \in \mathbb{Z}$ with $z^2 \equiv -1 \mod p$.

Let $r = \frac{z}{p}$ & $N = \lfloor \sqrt{p} \rfloor$. We apply the above lemma. Thus we find

$$\frac{s}{t} \in \mathbb{Q}, \quad \text{GCD}(s,t) = 1 \quad \text{s.t.}$$

$$\left| \frac{z}{p} - \frac{s}{t} \right| \leq \frac{1}{t(1+\lfloor \sqrt{p} \rfloor)} < \frac{1}{t\sqrt{p}}$$

and $t \leq \lfloor \sqrt{p} \rfloor < \sqrt{p}$.

Let $u = ps - zt$. As $t, p > 0$ we have

$$|u| = |ps - zt| = pt \left| \frac{z}{p} - \frac{s}{t} \right| < p \not{t} \frac{1}{\not{t}\sqrt{p}} = \sqrt{p}$$

Thus we obtain

1) $u^2 + t^2 < p + p = 2p$

2) $u^2 + t^2 = (ps - zt)^2 + t^2 \equiv z^2 t^2 + t^2 \mod p$

$$= (z^2+1)t^2 \equiv 0 \mod p.$$

$(z^2 \equiv -1)$

Thus $u^2+t^2 \in \mathbb{N}$ s.t. $p \mid u^2+t^2 < 2p$

Only possibility of u^2+t^2 is p. Thus $u^2+t^2 = p$. ☐

RMK: The above proof is constructive, and in fact, gives an algorithm to find solution of $x^2+y^2 = p$.

Hermite's algorithm

The steps in the above proof are the following:

1) Find z s.t. $z^2 \equiv -1 \bmod p$. Such z exists as $\left(\frac{-1}{p}\right) = 1$.

2) Compute n'th convergent $\frac{s_n}{t_n}$ of the continued fraction of $\frac{z}{p}$ such that $t_n < \sqrt{p} < t_{n+1}$.

3) Then $(x, y) = (ps_n - zt_n, t_n)$ is a solution of $x^2+y^2 = p$.

Ex 1: Solve $x^2 + y^2 = 13$.

(secretly, we know $2^2 + 3^2 = 13$)

Sol: Indeed, $\left(\frac{-1}{13}\right) = 1$. We check that $\left(\frac{2}{13}\right) = (-1)^{\frac{13^2-1}{8}} = (-1)^{\frac{14\times 12}{8}} = -1$.

Thus by Euler's criterion (week 4/5)

$$z = 2^{\frac{13-1}{4}} \bmod 13 = 8 \bmod 13.$$

$\Rightarrow z = \pm 5 \bmod 13$ is a solution to

$$z^2 \equiv -1 \bmod 13$$

Continued fraction of $\frac{5}{13} = [0; 2, 1, 1, 2]$

$a = 0$, $a_1 = \left\lfloor \frac{13}{5} \right\rfloor = 2$,

$$P_2 = \left(\frac{13}{5} - 2\right)^{-1} = \frac{5}{3}, \quad a_2 = 1$$

$$P_3 = \frac{1}{\frac{5}{3} - 1} = \frac{3}{2}, \quad a_3 = 1$$

$$P_4 = \frac{1}{\frac{3}{2} - 1} = 2 = a_4$$

$$\frac{s_1}{t_1} = [0; 2] = \frac{1}{2}, \quad \frac{s_2}{t_2} = [0; 2, 1] = \frac{1}{3}$$

$$\frac{s_3}{t_3} = [0; 2, 1, 1] = \frac{2}{5}.$$

Ans $3 < \sqrt{13} < 5$ $(9 < 13 < 25)$

we stop the algorithm.

$u = p s_n - 2 t_n = 13 \times 1 - 5 \times 3 = -2$

$t = 3 \Rightarrow (2, 3)$ is a solution.

Ex 2: Solve $x^2 + y^2 = 17$.

Ans: we check $\left(\frac{3}{17}\right) = -1$.

Indeed $\left(\frac{3}{17}\right)\left(\frac{17}{3}\right) = (-1)^{\frac{(17-1)(3-1)}{4}} = 1$

& $\left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1$.

Thus by Euler's criterion, $3^{\frac{17-1}{4}} = 3^4 \equiv -4 \mod 17$ is a solution. Take $z = 4$

Continued fraction of $\frac{4}{17} \Rightarrow a = 0$

$p_1 = \frac{17}{4} \Rightarrow a_1 = 4$, $p_2 = \frac{1}{\frac{17}{4} - 4} = 4 = a_2$

$\Rightarrow \frac{4}{17} = [0; 4, 4]$

$s_1 = [0; 4] = \frac{1}{4}$, $s_2 = [0; 4, 4] = \frac{4}{17}$

Indeed, $4 < \sqrt{17} < 17$. So $s_n = 1, t_n = 4$

$u = 4 \times 4 - 17 \times 1 = -1 \Rightarrow (1, 4)$ is a solution.