Lecture on sums of squares

Carl Löndahl

March 22, 2011

Question: Which integers n can be represented

$$n = a^2 + b^2$$

Lemma 1. *If*

$$m = a^2 + b^2, n = c^2 + d^2 \implies mn = x^2 + y^2$$

Proof. Set

$$z = a + bi, w = c + di$$

$$m = a^2 + b^2 = |a + bi|^2 = |z|^2, n = c^2 + d^2 = |c + di|^2 = |w|^2$$

$$mn = |z|^2|w|^2 = |(a+bi)(c+di)|^2 = |(ac-bd)+i(ad+bc)|^2 = (ac-bd)^2+(ad+bc)^2$$

□

Dirichlet's box lemma(Pigeonhole principle)

Lemma 2 (Thue)**.** *p prime, $a \in \mathbf{Z}$, $p \not| a$. Then*

$$ax \equiv y \pmod{p}$$

has solutions x_0, y_0 where

$$0 < |x_0| < \sqrt{p}, 0 < |y_0| < \sqrt{p}$$

Proof. Set $k = [\sqrt{p}] + 1$ and consider

$$f : \{0, 1, ..., k-1\} \times \{0, 1, ..., k-1\} \to \{0, 1, ..., k-1\}$$

$$(x, y) \mapsto ax - y \pmod{p}$$

□

with $k^2 > p$. By Dirichlets $\exists (x_1, y_1) \neq (x_2, y_2)$ s.t. $f(x_1, y_1) = f(x_2, y_2)$. Hence,

$$ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p}$$

$$a(x_1 - x_2) - (y_1 - y_2) \equiv 0 \pmod{p}$$

Now set $x_0 = x_1 - x_2$ and $y_0 = y_1 - y_2$. So

$$ax_0 - y_0 \equiv 0 \pmod{p} \iff ax_0 \equiv y_0 \pmod{p}$$

Since $\gcd(a, p) = 1$, $x_0 \equiv 0 \iff y_0 \equiv 0 \pmod{p}$. *Since $(x_1, y_1) \neq (x_2, y_2)$, we have that $x_0 \not\equiv 0$ and $y_0 \not\equiv 0 \pmod{p}$.*

Theorem 1 (Fermat)**.** *An odd prime p is a sum of two squares* $\iff$ $p \equiv 1 \pmod 4$.

Proof. (=¿) Assume $p = a^2 + b^2$, $a, b \in \mathbf{Z}$, $a, b > 0$. Then $p \not| a$ if $a = pk, k \geq 1$.

$$p = (pk)^2 + b^2 \geq p^2 k \geq p^2.$$

Contradiction! If $a = p0 = 0$, then $p = 0^2 + b^2 = b^2$. Contradiction! So $p \not| a$, $p \not| b$.

$$bx \equiv 1 \pmod p$$

has a solution $x = c$ s.t. $bx \equiv 1 \pmod p$.

$$c^2 | (a^2 + b^2)c^2 = pc^2 \equiv 0 \pmod p$$

$$(ac)^2 + (bc)^2 = (ac)^2 + 1 \pmod p \implies (ac)^2 \equiv -1 \pmod p \implies (-1/p) = 1 \implies p \equiv 1 \pmod 4$$

(¡=) Let $p \equiv 1 \pmod 4$. Then $(-1/p) = 1$ so $\exists a \in \mathbf{Z}$ s.t. $a^2 \equiv -1 \pmod p$. Then $a \neq 0 \pmod p$ so $p \not| a$. Thues lemma $\implies$

$$\exists x, y \in \mathbf{Z} : ax \equiv y \pmod p, 0 < |x_0| < \sqrt{p}, 0 < |y_0| < \sqrt{p}$$

□

Example 1. $p = 29 \equiv 1 \pmod 4$.

$$a^2 \equiv -1 \pmod{29}, \quad a = 12$$

$$(12)^2 = 144 = -1 \pmod{29}, 145 = 29 \times 5$$

$$12x \equiv y \pmod{29}, \quad 0 < |x_0| < \sqrt{29}, 0 < |y_0| < \sqrt{29}$$

Only fives cases, i.e. 1,2,...5 to try. Using trial-and-error we find that for $x = 2$ and $x = 5$ are -5 and 2, whose absolute values are less than $\sqrt{29}$. So $(x, y) = (2, -5)$. $y^2 \equiv (-5)^2 \equiv (12x)^2 \equiv 12^2 x^2 \equiv -x^2$

$$x^2 + y^2 \equiv 0 \pmod{29}, 2^2 + (-5)^2 = 29$$

Proposition 1. *A prime of the form $4k + 1$ can be represented uniquely (up to order of the summands) of a sum of two squares.*

Proof. Assume

$$p = a^2 + b^2 = c^2 + d^2, \quad a, b, c, d \in \mathbf{Z} > 0$$

Then $a^2 d^2 - b^2 c^2 = a^2 d^2 + b^2 d^2 - b^2 d^2 - b^2 c^2 = d^2(a^2 + b^2) - b^2(d^2 + c^2) = p(d^2 - b^2) \equiv 0 \pmod p$. So $p \mid a^2 d^2 - b^2 c^2 = (ad - bc)(ad + bc) \implies ad \equiv bc \mod p$ or $ad \equiv -bc \mod p$.

Now $0 < a, b, c, d < \sqrt{p} \implies 0 < ad, bc < p$ gives either

$$ad = bc \text{or} ad = -bc$$

Claim: $ad + bc = p \implies ac = bd$

$p^2 = (a^2+b^2)(c^2+d^2) = (ad+bc)^2+(ac-bd)^2 = p^2+(ac+bd)^2 \implies (ac+bd)^2 = 0$

By symmetry $(c <-> d)$ may assume

$$ad = bc$$

If $D = \gcd(a, b)$ then $D^2 \mid (a^2 + b^2) = p \implies D = 1 = \gcd(a, b)$

$$a \mid ad = bc \implies a \mid c, c = ka, \quad k \in \mathbf{Z}.$$

$$ad = bka \implies d = bk \quad (c, d) = k(a, b)$$

□

Theorem 2. *Let $n \in \mathbf{Z}$, $n > 0$, $n = N^2m$ with m square free. Then*

$$n = a^2 + b^2$$

m contains no prime factors of the form $4k + 3$.

Proof. (¡=) If $m = 1$, $n = N^2 = N^2 + 0^2$. Let $m > 1$, $m = p_1...p_n$. $p_i = 2$ or $p_i \equiv 1 \pmod 4$. By repeatedly using

$$(a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2$$

obtain

$$m = x^2 + y^2, \quad \exists x, y \in \mathbf{Z}$$

Then

$$n = N^2m = N^2(x^2 + y^2) = (Nx)^2 + (Ny)^2$$

(=¿) Assume that

$$n = a^2 + b^2 = N^2m$$

Let p be an odd prime dividing m

$$d = \gcd(a, b), \quad a = dr, b = ds, gcd(r, s) = 1$$

$$d^2(r^2 + s^2) = (dr)^2 + (ds)^2 = n = N^2m \implies d^2 \mid N^2$$

if $m = tp$

$$r^2 + s^2 = (N^2/d^2)m = (N/d)^2tp \implies r^2 + s^2 \equiv 0 \pmod p$$

So $\gcd(r, s) = 1 \implies p \not| r$ or $p \not| s$. Say (wlog!) $p \not| r$.

$$\exists r' \in \mathbf{Z} : rr' \equiv 1 \pmod p$$

which gives

$$r'^2(r^2 + s^2) = (rr')^2 + (sr')^2 \equiv 0 \pmod p \implies 1 + (r's) \equiv 0 \pmod p$$

So $(-1/p) = 1$ which is true iff $p \equiv 1 \pmod 4$

□

Theorem 3. *$n \in \mathbf{Z}$ can be written*

$$n = a^2 - b^2, \quad a, b \in \mathbf{Z} \iff n \not\equiv 2 \pmod 4$$

Proof. (=¿) As

$$a^2, b^2 \equiv 0, 1 \pmod 4$$

So

$$a^2 - b^2 \equiv 0, 1, 3 \pmod 4$$

which is never equivalent to 2. So if $n \equiv 2$ the form above if impossible!

(¡=) Let first $n \equiv 1$ or 3 $\pmod 4) implies n+1, n-1$ even.

$$\left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 = \left(\frac{n+1}{2} + \frac{n-1}{2}\right)\left(\frac{n+1}{2} - \frac{n-1}{2}\right) = n$$

Let next $n \equiv 0 \pmod 4$ so that $n/4 \in Z$

$$(n/4+1)^2 - (n/4-1)^2 = \left(n^2/16 + n/2 + 1\right) - \left(n^2/16 - n/2 + 1\right) = n$$

□