We start the course with examples on how to solve (certain) Diophantine equations

$$P(x) = 0 \quad , \quad x \in \mathbb{Z}^n \quad , \quad P \in \mathbb{Z}[X_1, \dots, X_n].$$

Example 1:

Theorem (Fermat)

Let $n \in \mathbb{Z} - \{0\}$. Then

$$n = a^2 + b^2 = \square + \square \qquad (a, b \in \mathbb{Z})$$

iff (i) $n > 0$

(ii) $n = m^2 r$, where $r = \prod_{i=1}^{k} p_i$ for $k \geq 0$ and $p_i \in \mathbb{N}$ distinct primes satisfying $p_i \equiv 1, 2 \bmod (4)$.

In particular, if $p \in \mathbb{N}$ is prime, then

$$p = \square + \square \iff p \equiv 1, 2 \bmod (4)$$

Remark: $n = \square + \square \iff \exists z \in \mathbb{Z} + i\mathbb{Z} \subseteq \mathbb{C}$ s.t. $n = z\bar{z} = |z|^2$.

$\mathbb{Z} + i\mathbb{Z} \Rightarrow$ Gaussian integers

The Gaussian integers

Proposition

- $\mathbb{Z}+i\mathbb{Z} = \{a+ib : a,b\in\mathbb{Z}\} < \mathbb{C}$ is a subring (called the Gaussian integers).
- We have $\mathbb{Z}+i\mathbb{Z} = \mathbb{Z}[i] := \{P(i) : P\in\mathbb{Z}[X]\}$ ← smallest subring of $\mathbb{C}$ containing $\mathbb{Z}$ and i
- $\mathbb{Z}+i\mathbb{Z}$ is a domain and ← smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and i

$$\mathrm{Frac}(\mathbb{Z}+i\mathbb{Z}) = \mathbb{Q}(i) = \mathbb{Q}[i] = \mathbb{Q}+i\mathbb{Q}$$ (the field of Gaussian numbers)

Proof:

- $\mathbb{Z} < \mathbb{Z}+i\mathbb{Z} < \mathbb{C} \Rightarrow 0,1 \in \mathbb{Z}+i\mathbb{Z}$
- $(a+ib)(c+id) = (ac-bd)+i(ad+bc) \in \mathbb{Z}+i\mathbb{Z}$

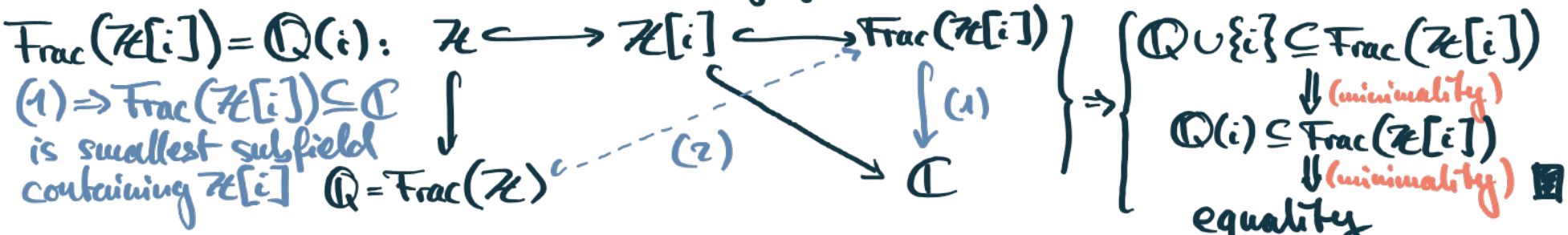
$\Rightarrow$ $\mathbb{Z}+i\mathbb{Z}$ is a subring of $\mathbb{C}$ containing $\mathbb{Z}$ and i.

- Clearly $\mathbb{Z}+i\mathbb{Z} \subseteq \mathbb{Z}[i]$. Minimality gives equality. (alternative: $i^2=-1 \Rightarrow P(i)\in\mathbb{Z}+i\mathbb{Z}$)
- Same argument $\Rightarrow$ $\mathbb{Q}+i\mathbb{Q} = \mathbb{Q}[i] \subseteq \mathbb{Q}(i)$
- $x = a+ib \in \mathbb{Q}[i]-\{0\} \Rightarrow y = \frac{a-ib}{a^2+b^2} \in \mathbb{Q}[i]$ is an inverse, i.e. $xy=1$.

$\Rightarrow \mathbb{Q}[i]^\times = \mathbb{Q}[i]-\{0\}$

$\Rightarrow \mathbb{Q}[i]$ is a field and minimality gives $\mathbb{Q}[i] = \mathbb{Q}(i)$

- $\mathrm{Frac}(\mathbb{Z}[i]) = \mathbb{Q}(i)$:



(1) $\Rightarrow \mathrm{Frac}(\mathbb{Z}[i]) \subseteq \mathbb{C}$ is smallest subfield containing $\mathbb{Z}[i]$

$\Rightarrow$ $\mathbb{Q}\cup\{i\} \subseteq \mathrm{Frac}(\mathbb{Z}[i])$

$\Downarrow$ (minimality)

$\mathbb{Q}(i) \subseteq \mathrm{Frac}(\mathbb{Z}[i])$

$\Downarrow$ (minimality)

equality ∎

Remark: $\mathbb{Q}(i) \cong \mathbb{Q}[X]/(X^2+1)$ admits two embeddings in $\mathbb{C}$: $a+ib \mapsto a+ib \in \mathbb{C}$ and $a+ib \mapsto a-ib \in \mathbb{C}$,

i.e. $z \mapsto \bar{z}$ restricts to the non-trivial Galois automorphism on $\mathbb{Q}(i)$.

Definition:

The norm on $\mathbb{Q}(i)$ is the map

$$z \mapsto N_r(z) = z\bar{z} = \prod_{\sigma \in Gal(\mathbb{Q}(i)|\mathbb{Q})} \sigma(z).$$

Proposition

N_r is $\mathbb{Q}$-valued, multiplicative, definite (i.e. $N_r(z)=0 \Leftrightarrow z=0$) and $N_r(\mathbb{Z}[i]) \subseteq \mathbb{N} \cup \{0\}$.

equality is false, by Fermat's theorem

[Multiplicativity: $\overline{z_1 z_2} = \bar{z}_1 \cdot \bar{z}_2$ for any $z_1, z_2 \in \mathbb{C}$. The rest is clear.]

Proposition

$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} = \{z \in \mathbb{Z}[i] : N_r(z) = 1\}$

Proof: Let $z \in \mathbb{Z}[i] - \{0\} \Rightarrow z^{-1} \in \mathbb{Q}(i)$ exists and

$$1 = N_r(z^{-1}z) = N_r(z^{-1}) N_r(z) \Rightarrow N_r(z^{-1}) = N_r(z)^{-1}.$$

($N_r(z) \in \mathbb{Z} - \{0\}$)

Thus $z^{-1} \in \mathbb{Z}[i] \Rightarrow N_r(z)^{-1} \in \mathbb{Z} \to N_r(z) \in \{\pm 1\} \cap N_r(\mathbb{Z}[i]) = \{1\}$.

$\therefore z \in \mathbb{Z}[i]^\times \Rightarrow N_r(z) = 1$

o.t.o.h. $N_r(z) = 1 \Rightarrow \bar{z} = \frac{1}{N_r(z)} z \in \mathbb{Z}[i]$.

This proves $\mathbb{Z}[i]^\times = \{z : N_r(z) = 1\}$. Now solve $a^2+b^2=1$.

∎

Corollary If $n_1, n_2 \in \mathbb{Z}$ s.t. $n_i = \square + \square$, then $n_1 n_2 = \square + \square$

Proof: $n_i = Nr(z_i)$ for some $z_i \in \mathbb{Z}[i]$, thus

$$n_1 n_2 = Nr(z_1)N(z_2) = Nr(z_1 z_2) = \square + \square.$$

Remark: opposite is false: $9 = \square + \square$ but $3 \neq \square + \square$.

Proposition (partial converse)

If $n_1, n_2 \in \mathbb{N}$ are coprime, then

$$n_1 n_2 = \square + \square \implies n_i = \square + \square \text{ for both } i = 1, 2.$$

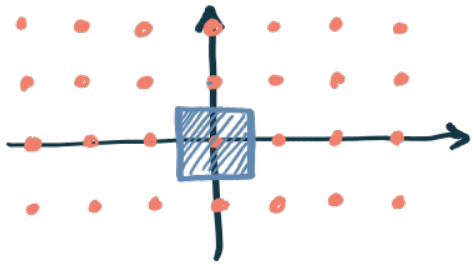
Proof later

Proposition (unique factorization in $\mathbb{Z}[i]$)

$\mathbb{Z}[i]$ is a PID, i.e., a domain and every ideal $I \lhd \mathbb{Z}[i]$ is of the form $I=(q)$ for some $q \in \mathbb{Z}[i]$

Proof: **Step 1**: $\mathbb{Z}[i]$ is euclidean (stronger): $\mathbb{Z}\left[\frac{1}{2}(1+\sqrt{-19})\right]$ is PID, not Euclidean.

$\forall z, q \in \mathbb{Z}[i], q \neq 0 \ \exists k, r \in \mathbb{Z}[i]$ s.t. $Nr(r) < Nr(q)$ and $z = kq + r$.



$\Rightarrow$ every $s \in \mathbb{C}$ is of the form $s = g + k$ with $k \in \mathbb{Z}[i]$ and $|g| \leq \frac{\sqrt{2}}{2} < 1$.

$\therefore \exists k \in \mathbb{Z}[i]$ s.t. $\left|\frac{z}{q} - k\right| < 1$.

Let $r = z - kq$, then $z = kq + r$ and

$$Nr(r) = |r|^2 = |z - kq|^2 = \left|\frac{z}{q} - k\right|^2 |q|^2 < |q|^2 = N(q).$$

Step 2: $\mathbb{Z}[i]$ is a PID:

Let $I \lhd \mathbb{Z}[i]$. If $I = \{0\}$, we are done. So w.l.o.g. $I \neq \{0\}$.

$\Rightarrow \exists q \in I$ of minimal norm.

Let $z \in I$, then $z = kq + r$ with $Nr(r) < N(q)$. Thus

$$r = z - kq \in I \Rightarrow Nr(r) = 0.$$

$\Rightarrow \forall z \in I \ \exists k \in \mathbb{Z}[i] \ z = kq \iff I = (q)$.

Proposition

Let $q \in \mathbb{Z}[i] - \{0\}$. Then

$$\left| \mathbb{Z}[i]/(q) \right| = Nr(q)$$

and, in particular, $\mathbb{Z}[i]/(q)$ is finite.

Proof: We identify $\mathbb{Z}[i] \xrightarrow{\vartheta} \mathbb{Z}^2$ via the choice of the basis $(1,i)$. If $q \in \mathbb{Z}[i]$, then

$$[\times q] : \mathbb{Z}[i] \longrightarrow \mathbb{Z}[i], \quad z \mapsto zq$$

is a $\mathbb{Z}$-linear map and this gives rise to a ring homomorphism

$$i : \mathbb{Z}[i] \hookrightarrow Mat_2(\mathbb{Z}),$$

s.t. $\forall z, q \in \mathbb{Z}[i]$ $\vartheta(zq) = \vartheta(z) i(q)$. $(q \neq 0 \Rightarrow i(q) \in GL_2(\mathbb{Q}))$

Note that for $q = a + ib$ we have

$$\left.\begin{aligned} (a,b) = \vartheta(q) = \vartheta(1) i(q) = (1,0) i(q) \\ (-b,a) = \vartheta(iq) = \vartheta(i) i(q) = (0,1) i(q) \end{aligned}\right\} \Rightarrow i(q) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Also, we note that $\vartheta((q)) = \mathbb{Z}^2 i(q)$. Therefore

$$\mathbb{Z}[i]/(q) \cong \mathbb{Z}^2 / \mathbb{Z}^2 \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

and $\left[\mathbb{Z}^2 : \mathbb{Z}^2 \begin{pmatrix} a & b \\ -b & a \end{pmatrix}\right] \overset{(*)}{=} \left| \det \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \right| = a^2 + b^2 = Nr(q)$ $\overset{(**)}{}$

∎

Proof of partial converse: Let $m,n \in \mathbb{N}$ coprime and $a,b \in \mathbb{N}$ s.t. $mn = a^2+b^2$, i.e.

$$mn = Nr(a+ib). \quad (*)$$

Set $q = a+ib$. $(*)$ shows that

$$(mn) = (q\bar{q}) = (q).(\bar{q}) = (q).\overline{(q)}.$$

Goal: Find $\underline{b} \lhd \mathbb{Z}[i]$ s.t. $(m) = \underline{b}.\overline{\underline{b}}$. As $\mathbb{Z}[i]$ is a PID, it follows that $\underline{b} = (r)$ for some $r \in \mathbb{Z}[i]$ and thus $(m) = (r).\overline{(r)} = (r\bar{r}) = (Nr(r))$. This implies that there is $\varepsilon \in \mathbb{Z}[i]^\times$ s.t. $m = \varepsilon Nr(r)$. But $m, Nr(r) \in \mathbb{N} \Rightarrow \varepsilon = 1$. Similar for n.

Note that $(m),(n) \lhd \mathbb{Z}[i]$ are coprime, as $1 = sm+tn$ for some $s,t \in \mathbb{Z}$ (Bézout) $\Rightarrow 1 \in (m)+(n)$.

Let $\underline{a} = (q)$, then

$$(m).(n) = \underline{a}.\overline{\underline{a}} \qquad \left((m).(n) = (mn) = (Nr(q)) = (q\bar{q}) = (q).(\bar{q}) = (q).\overline{(q)} = \underline{a}.\overline{\underline{a}}\right)$$

and therefore

$$(\underline{a},(m)).(\underline{a},(n)) = (\underline{a}+(m)).(\underline{a}+(n)) \qquad \left(\text{Note } (S)+(T) = ((S)\cup(T)) = (S\cup T)\right)$$

$(\underline{a},(m))$: ideal generated by $\underline{a}$ and (m) $= \underline{a}+(m)$. This is the ideal $\underline{b}$.

$$= \underbrace{\underline{a}^2}_{\subseteq \underline{a}} + \underbrace{\underline{a}((m)+(n))}_{=\underline{a}} + \underbrace{(m).(n)}_{\subseteq \underline{a}} = \underline{a}$$

and similarly $\overline{\underline{a}} = (\overline{\underline{a}},(m)).(\overline{\underline{a}},(n))$.

Note: $\overline{(m)} = (m) \Rightarrow (\overline{\underline{a}},(m)) = (\overline{\underline{a}},\overline{(m)}) = \overline{(\underline{a},(m))}$.

Claim: Let $\underline{b} = (\underline{a}, (m))$, then $(m) = \underline{b}.\overline{\underline{b}}$.

$$\underline{b}.\overline{\underline{b}} = (\underline{a} + (m)).(\overline{\underline{a}} + (m)) = (mn) + (\underline{a} + \overline{\underline{a}}).(m) + (m)^2$$

$$= \underbrace{(\underline{a} + \overline{\underline{a}})(m)}_{\subseteq (m)} + \underbrace{((n) + (m))}_{= \mathbb{Z}[i]}(m) = (m).$$

Similarly, one finds that $\underline{e} = (\underline{a}, (n)) \Rightarrow (n) = \underline{e}.\overline{\underline{e}}$.

∎

Proof of Fermat's two squares theorem:

We want to determine when $n = \square + \square$. Clearly, n has to be non-negative. If $n=0$, the statement is clear. Also, we can assume that n is square-free, i.e., if p is a prime and $p \mid n$, then $p^2 \nmid n$. Using the partial converse, we only need to determine when

$$p = \square + \square.$$

Note that $2 = 1^2 + 1^2 = \square + \square$, so from now on w.l.o.g. p is odd.

Theorem:

Let p an odd prime. TFAE:

(1) $p = \square + \square$

(2) $p \equiv 1 \bmod (4)$

(3) $-1 \equiv \square \bmod (p)$

(1)⇒(3): $p = a^2 + b^2 \Rightarrow 1 = (a,b)(p,ab)$ (note: $p \mid a \Rightarrow p \mid b$ and $p^2 \mid a^2 + b^2$).

$\Rightarrow a$ is a unit mod p

Therefore $b^2 \equiv -a^2 \bmod (p)$

$\Rightarrow -1 = \underbrace{b^2 \tilde{a}^2}_{=(b\tilde{a})^2} \bmod (p)$, where $\tilde{a}a \equiv 1 \bmod (p) \Rightarrow (3)$.

(3)⇒(2): $\alpha \in \mathbb{F}_p^\times$ s.t. $\alpha^2 = -1 \Rightarrow \operatorname{ord}(\alpha) = 4$ (as $\operatorname{char}(\mathbb{F}_p) \neq 2$).

Now $\operatorname{ord}(\alpha) \mid |\mathbb{F}_p^\times| = p-1 \Rightarrow (2)$. (Lagrange's theorem)

(2) $\Rightarrow$ (3): $4 \mid p-1$ and $\mathbb{F}_p^\times$ cyclic $\Rightarrow \mathbb{F}_p^\times$ has a cyclic subgroup $L = \langle \beta \rangle$ of order 4.

[$\mathbb{F}_p^\times = \langle \alpha \rangle$, $|\mathbb{F}_p^\times| = 4k \Rightarrow |\langle \alpha^k \rangle| = 4$]

Thus $(\beta^2)^2 = 1$, $\beta^2 \neq 1 \Rightarrow \beta^2 = -1$ in $\mathbb{F}_p \Rightarrow$ (3).

(3) $\Rightarrow$ (1): Suppose $\alpha \in \mathbb{F}_p$ s.t. $\alpha^2 = -1$. Let $m \in \mathbb{Z}$ s.t. $m \equiv \alpha \bmod (p)$. Then

$$p \mid m^2 + 1.$$

Recall Euler's descent step from general introduction: $p \mid \square + \square \Rightarrow p = \square + \square$ (coprime).

Let $q = m + i$ and note that $m^2 + 1 = q\bar{q} \in (p)$ but $q \notin (p)$

$$\Rightarrow \mathbb{Z}[i]/(p) \text{ has zero-divisors,}$$

i.e. (p) is not prime $\iff$ p is not irreducible.

Let $r \in \mathbb{Z}[i]$ irreducible s.t. $r \mid p$ $(r \notin \mathbb{Z}[i]^\times)$.

Note: $r \mid p \Rightarrow \bar{r} \mid \bar{p} = p$ i.e. p is divisible by both r and $\bar{r}$.

Moreover, $\bar{r} \notin \mathbb{Z}[i]^\times r$ (i.e. $(r) \neq (\bar{r}) = \overline{(r)}$).

[$r = \xi \bar{r}$

$a + ib = a - ib \Rightarrow b = 0 \Rightarrow p \in (a) \Rightarrow \mathrm{Nr}(a) \mid N(p) \Rightarrow a^2 \mid p^2 \Rightarrow a \in \{\pm 1, \pm p\}$

This is absurd as $r \in \mathbb{Z}[i] - \mathbb{Z}[i]^\times$ is irreducible by assumption.

$a + ib = -a + ib \Rightarrow a = 0 \Rightarrow p \in (b) \Rightarrow$ same argument as above.

$a+ib = i(a-ib) = b+ia \Rightarrow a=b \Rightarrow r = a(1+i) \Rightarrow 2a^2 = Nr(1+i)a^2 \mid p^2$ ↯

$a+ib = -i(a-ib) = -b-ia \Rightarrow a=-b \Rightarrow r = a(1-i) \Rightarrow 2a^2 \mid p^2$ ↯

Let $\pi = (r)$. As $\pi \mid (p)$ (i.e. $(p) \subsetneq \pi$), we find

$$\mathbb{Z}[i]/(p) \xrightarrow{\Phi} \mathbb{Z}[i]/\pi$$

a ring homomorphism with non-trivial kernel (as π is prime by irreducibility of r). Moreover, the RHS is non-trivial as $\pi \neq \mathbb{Z}[i]$ (because r is not a unit).

Therefore

$$1 < Nr(r) = \left|\mathbb{Z}[i]/\pi\right| = \frac{\left|\mathbb{Z}[i]/(p)\right|}{|\ker \Phi|} < \left|\mathbb{Z}[i]/(p)\right| = Nr(p) = p^2$$

and therefore $Nr(r) = p$, i.e. $p = \square + \square$.

∎

Fermat's equations and Fermat's last theorem:

We call the family of Diophantine equations

$$X^n + Y^n = Z^n \qquad (n \geq 2)$$

($n=1$ is really easy.)

Fermat's equations.

Theorem (Pythagorean triples)

For $n=2$, a triple $(x,y,z) \in \mathbb{Z}^3$ is a non-trivial (e.g. $(1,0,1)$) primitive solution to Fermat's equation (i.e. a primitive Pythagorean triple) iff there are $u,v \in \mathbb{Z}$ coprime s.t.

$$(x,y,z) = \pm(u^2-v^2, -2uv, u^2+v^2).$$

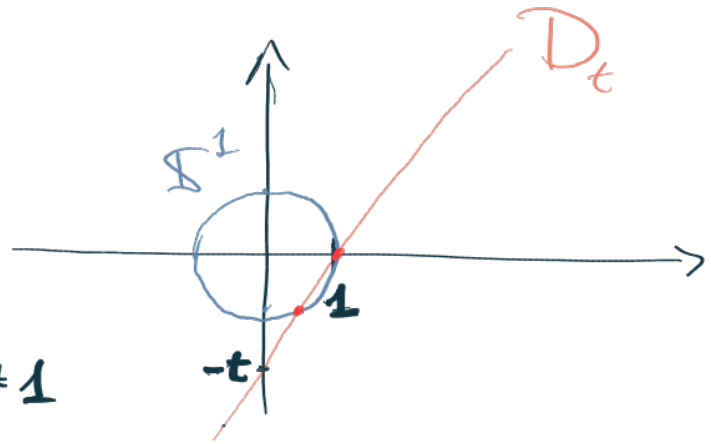
In particular, there are infinitely many primitive solutions.

Proof: We first show a procedure to construct a solution.

(i) Let $t \in \mathbb{Q}$ and let $u, v \in \mathbb{Z}$ s.t. $t = \frac{u}{v}$ is reduced.

Let $D_t = \{(A,B) \in \mathbb{R}^2 : B = tA - t\}$

$= \{B = t(A-1)\}$



(ii) Note that $D_t \cap \mathbb{S}^1 = \{(1,0), (A,B)\}$ with $A \neq 1$ and $A^2 + B^2 = 1$.

(iii) A calculation shows

$$(A,B) = \left(\frac{t^2-1}{t^2+1}, -\frac{2t}{t^2+1}\right) = \left(\frac{u^2-v^2}{u^2+v^2}, -\frac{2uv}{u^2+v^2}\right)$$

(iv) One checks that

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

is a primitive Pythagorean triple.

Now, given a non-trivial primitive solution (x,y,z) (w.l.o.g. $z > 0$), let $(A,B) = \left(\frac{x}{z}, \frac{y}{z}\right)$ and and note that $A^2 + B^2 = 1$, $|A| < 1$. One checks that the line

$$D_{\frac{y}{x-z}} = \left\{(U,V) \in \mathbb{R}^2 : V = \frac{y}{x-z}(U-1)\right\}$$

passes through (A,B) and $(1,0)$.

This shows that up to sign every non-trivial primitive solution is obtained via the initial procedure.

The situation is very different for $n \geq 3$!

Fermat's last theorem (Wiles '95)

For $n \geq 3$, Fermat's equation does not admit any non-trivial integral solutions.

We will see: suffices to prove for $n = 4$ and n prime.

Famous special cases are due to Fermat ($n=4$), Euler ($n=3$), Legendre and Dirichlet ($n=5$), Lamé ($n=7$), Kummer (for all regular primes p, i.e. pth $\mathbb{Q}(\zeta_p)$, where $\zeta_p = e^{2\pi i/p}$).

conjecturally many ($\sim 60\%$)
NOT known